LEARNING MADE EASY

Cryptomathic Special Edition

Digital Signatures

for dummies®
A Wiley Brand

Explore business and technical implications

Understand established regulatory standards

Deploy and manage digital signatures

Brought to you by:

CRYPTOMATHIC

Chris Allen

Steve Marshall

About Cryptomathic

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud, and mobile. With more than 30 years' experience, Cryptomathic provides systems for authentication, digital signatures, EMV issuing and authorization, key/crypto management, and PKI/ID, through best-of-breed security solutions and services.

www.cryptomathic.com

Digital Signatures

Cryptomathic Special Edition

by Chris Allen and Steve Marshall

for dummies®
A Wiley Brand

Digital Signatures For Dummies®, Cryptomathic Special Edition

Published by: **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate

Chichester, West Sussex, www.wiley.com

Registered Office

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-42289-1 (pbk), ISBN 978-1-119-42290-7 (ebk)

Printed in Great Britain

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner

Editorial Manager: Rev Mengle

Executive Editor: Katie Mohr

Business Development Representative: Frazer Hossack

Production Editor: Siddique Shaik

Cryptomathic Project Manager: Stefan Hansen

Table of Contents

Introduction

We're living in the Digital Age, in which every day most people complete some digital task (or, even more likely, *many* digital tasks) that used to be done on paper. It may come as a surprise to learn that digital signatures, the electronic counterpart of handwritten signatures, were a new idea not recently, but four decades ago.

The concept was first advanced in the mid-1970s, proposing that a "digital or electronic signature" could be applied to a "digital message" so that the recipient would be able to validate the authenticity and integrity of that message. The aim was to prove that the message sent was genuine and hadn't been altered. A digital signature would depend upon strong cryptography and solid techniques.

Great idea, but who would use it, and for what? There just wasn't enough genuine demand from commercial businesses or governments for the additional level of "trust" that these digital signatures could provide. What, pray tell, was wrong with paper, traditional signatures, seals, and the postal service? Digital signatures were a technical solution waiting for a problem to solve.

It's 40 years later now. Digital documents are increasingly commonplace, as are cross-border transactions. Almost every organization needs its own digital strategy, and those that are enlightened will deploy digital signatures as a part of that strategy, a demonstration of digital professionalism.

About This Book

Digital Signatures for Dummies, Cryptomathic Special Edition, is all about navigating this world that has finally arrived, a world where there is genuine market demand to use digital signatures in support of business and organizational goals. This book is a guide for appreciating, considering, and understanding the commercial and technical factors required to manage and deploy these techniques.

This book outlines the benefits of embracing digital signature techniques within your digital strategy and demystifies the

relevant technologies. It places these techniques in context with other recent IT developments and puts their history into a business perspective. Read on and you'll learn more about technical interoperability and the continued development and evolution of technical standards pertaining to digital signatures. You'll come away with valuable guidance, insights, and pointers accumulated from decades of the authors' experiences in developing and implementing these technologies.

If you're interested in digitally signing and distributing "stuff" — including electronic documents, for sure, but potentially also including software — you're likely to find helpful information in these pages. It's vital to get things right in the production and management of digital signatures, and your organization must fully consider all the pertinent technical, procedural, and regulatory requirements, both now and in the future.

With that in mind, the book includes plenty of descriptions of the various types of digital signatures, as well as the rules, regulations, and requirements associated with them. You'll find sufficient technical content and associated descriptions to get a genuine and overall appreciation of what's required to deploy and manage digital signatures.

Even if you're not digitally signing and distributing the kind of "stuff" we've mentioned, your organization still might be on the receiving end of increased volumes of digital signatures. If that's the case, you need to appropriately consider the classification, management, and retention of these kinds of documents, and that isn't always easy.

This book sets out to provide you, the reader, with valuable insights into the fast-expanding area of digital signature deployment and management. You may wish to view it as your initial guidebook. Like all guidebooks, it's likely to require revision and enhancements as the rules, regulations, and compliance requirements evolve.

This a guidebook, yes, but not necessarily a playbook or recipe book. Lots of pieces and parts make up a sound digital signature deployment, too many to fit in a guidebook of this size. But you'll have the basics, and obtain a good idea of the kinds of expertise to consult and the types of questions to ask as you proceed down this path.

Foolish Assumptions

It's always good to know the audience — this is what we're presuming about you, the reader who has opened this book:

- You're a businessperson or IT professional involved in the development and management of your organization's digital services.
- You need to understand the basics of deploying cryptographic services into IT systems, regardless of whether your perspective is technical or business-related.
- Your organization might be small and relatively simple, or bigger and more complex. Either way, you'll find practical pointers here.

Icons Used in This Book

Throughout this book, in the margins, you'll notice some natty little eye-catching icons. They decorate the page nicely, but they're more than just pretty faces. Here's what they signify:

REMEMBER

All of the book's pages offer lots of information, but the paragraphs next to this icon contain the details that are most significant.

TIP

Would you like a handy pointer that will help you on the road toward deployment of digital signatures? Look no further!

TECHNICAL STUFF

Just about anything related to IT security has the potential to be complicated and seriously technical. If the technical details are of interest to you, you'll find them close to this icon.

WARNING

Another thing that goes hand-in-hand with security measures is the possibility that something could go wrong. This icon points out some advice to avoid the potential pitfalls.

Where to Go from Here

If you're familiar with "For Dummies" books, you know that you're not necessarily expected to do things in the most predictable, ordinary way. Sure, start at the beginning and read all the way through! Or, if you prefer, pick and choose your content, because each chapter is written to stand alone, with enough context provided.

Of course, reading the whole book (or at least a few chapters) is the best way to get the most balanced and comprehensive appreciation of the business and technical influences of digital signatures, and the most important implications. But you'll come away with valuable insights no matter how many pages you turn, so read on!

IN THIS CHAPTER

- Introducing digital signatures
- Exploring the significance of digital signatures
- Understanding the importance of rules and standards

Chapter 1
Why Digital Signatures Are Relevant Now

People have used signatures for about as long as they've communicated beyond the spoken word — starting with handprints accompanying cave paintings. Signatures add everything from a touch of personal sentiment on a greeting card to a certification of authenticity on a painting to a binding agreement on a contract.

Digital signatures take the concept to a whole new level, as society's communications and business transactions move from physical representations to bits and bytes. U.S. President Ronald Reagan was famous for citing a Russian proverb that advised "trust but verify" — a digital signature does both. This chapter spells out some of the reasons for using digital signatures, explores how the concept has evolved, and explains how rules and standards make the world of digital signatures work.

Why Use Digital Signatures?

Organizations are now bringing online a lot of items that historically have been offline. Enormous savings are possible for government, companies, individuals, and the environment if it's

possible to communicate — and also commit and be held liable — electronically rather than on paper.

Here are some of the things digital signatures can do:

- Serve as an enabler for a business's digital strategy
- Provide non-repudiation with the strongest legal value
- Offer "what you see is what you sign" functionality
- Create a legally binding commitment
- Ensure enhanced security
- Provide end-user convenience and mobility
- Offer cost efficiency for all stakeholders

As shown in Figure 1-1, the benefits of digital signatures add up to convenience, security, and efficiency.

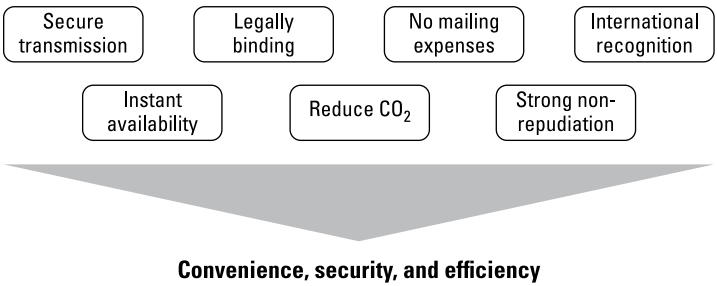

FIGURE 1-1: Reasons to use digital signatures.

Every organization determines its strategic priorities: perhaps speed to market and service, or maybe operating cost reduction. Those priorities provide the motivation for using digital signatures now.

REMEMBER

Today's world is online, and if your organization is online, you need to be professional with your online presence. You need to demonstrate how much you care about the quality of those services; one way is through the use of digital signatures.

It's a competitive world out there, and everyone wants to obtain a competitive advantage. It's best if digital signatures are seen as your advantage, and not your competitor's.

A SIGN OF TRUST

A digital signature provides trust. Some have likened it to a seal on a letter, which is a time-honored symbol designed to create trust in a paper document, but it's a whole lot more than that. The trust a digital signature brings can take a number of forms, best illustrated by example.

An organization wants to send out a tender document to selected companies, asking them to bid for a range of services. Such documents are often regarded as confidential or sensitive. If that's the case, the document would probably be encrypted and sent to the specified recipients, who would be provided with the encryption key needed to read the document.

But what if this organization specifically does not want to send this tender document out encrypted? Say it's a public-sector body wanting to demonstrate transparency? Maybe encryption is not appropriate, but it's still necessary to demonstrate the document is "authentic" with a source of origin that can be traced. It's also important to certify that the document is complete and that it hasn't been modified en route to its recipients.

The use of a digital signature achieves these objectives. Within the tender, data such as tender dates, quantity measurements, and quality considerations are all details that responding organizations must be able to rely upon. This trust is established by encrypting the tender document with a *private key,* which the responding companies can verify using the corresponding public key.

A Tool for Building Confidence

Digital signatures have been available since the mid-1970s and started being deployed into business services in the late 1980s. Usage at scale started some years later, but the concept did not catch on as quickly as anticipated, compared to digital services overall. Has the tide now turned forever? It certainly seems so.

Digital signatures are about trust. Within the past decade, billions of consumers have become comfortable spending time and transacting business online, using multiple device types. This requires trust so it isn't surprising that take-up, usage, and interest in digital signatures is now, at long last, growing.

REMEMBER

Digital communication and digital business are now natural and mainstream — services pretty much have to be online. Digital services are commercially critical in order to satisfy customer demands quickly and economically. What's more, today's consumers expect such services to be not only prompt, but also convenient and easy to use.

Banks, in particular, are driving everything online, making major reductions in their physical presence. Their efforts are due in large part to evaporating footfall.

At the same time, there's an ever-growing range of cybersecurity threats and scams making the headlines, and that is a destabilizing factor for everyone. Organizations appear to believe they have adequate disaster-recovery options in place to help them deal with major actual or perceived challenges. The resilience of online systems and services matters like never before, and is taken for granted by the majority of consumers who are frustrated when technology malfunctions.

When correctly deployed, digital signatures can be among the range of valuable, confidence-lifting countermeasures available to businesses operating in the ultra-digital landscape. The value of a digital signature is dependent upon sound implementation and management of cryptographic techniques. This requires discipline and rules to ensure interoperability with existing systems.

Rules of the Game

It takes teamwork and partnership to make technology adoption run and grow smoothly. To use digital signatures successfully for a prolonged period of time, you've got to get business and technical considerations to work in harmony. That's easy to say, but rather difficult to accomplish and sustain for years or even decades.

REMEMBER

In a word, it takes *rules.* To get the level of trust you're seeking from digital signatures, it takes a set of widely recognized and accepted rules.

Those who live or do business in the European Union know the EU loves its rules, and with so many member states transacting business with one another, it needs those rules. In the case of digital or electronic signatures, the EU saw the value early on.

The European Parliament issued Directive 1999/93/EC in — you guessed it! — 1999, providing a great start on a Community Framework for Electronic Signatures. This directive was well intentioned and should have encouraged the use and take-up of digital signatures. But it didn't.

Why didn't it work out? A big reason is that 1999/93 didn't require EU members to use common technical standards. There wasn't the cooperation or technical interoperability to make cross-border electronic transactions practical. By contrast, the adoption of chip payment cards shows how interoperability can lead to success.

So, maybe 1999/93/EC didn't get it right first time, but that didn't matter much because the marketplace wasn't ready to accept and adopt the technology, anyway. Consumer confidence and take-up of online services was in its infancy. Remember, this was more than three years before the launch of Facebook, and seven and a half before the launch of the iPhone!

TECHNICAL STUFF

Fast-forward 15 years or so, when 1999/99/EC was superseded by regulation 910/2014, focusing on electronic identification and trust services for electronic transactions in the internal market. This eIDAS Regulation was published in July 2014 and became internal market-effective two years later. Member states were given until July 1, 2017 to migrate to this new regulation.

Digital signatures have now been reenergized. There's a desire and commitment to put the technology and supporting services to work. Consumers have the technology available now, they can use it, and they do!

REMEMBER

They way this story has unfolded reflects a truth in the wider discipline of cryptography, when applied to business and everyday life. Cryptography used to be the responsibility of a few people in the IT department. These days, cryptography matters to business like never before.

WARNING

The use of digital signatures and cryptography can provide major business opportunities and benefits, but can also introduce unforeseen development and managerial issues. Such issues can, in turn, give rise to significant but unexpected costs and constraints for your business, often years after the original decisions were taken. That's a very good reason to use the products and services of vendors that have a proven track record of experience and knowledge.

EMV CHIP CARDS AND INTEROPERABILITY

Almost everyone uses credit or debit cards, and many people have several. They're ideal for buying everything from a coffee to a major appliance or even a car. But those extra-secure cards with embedded chips have taken a good while to become commonplace, and they would not have without solid technical (interoperability) standards.

Payment chip cards were introduced domestically in France in early 1990s. Later, international card schemes combined to develop the EMV framework/specification for global use. The United Kingdom (UK) introduced them in late 1997, started national rollout in 2003, and has moved onto EMV-based contactless cards. Still, EVM payment cards retain their magnetic stripe and have embossed details. Why? To allow global interoperability.

EMV is global, and chip cards are used in Europe, Asia, and Australia, plus the United States and Canada. But it has taken more than 20 years to reach its current maturity.

What drivers contributed to chip card adoption? First, commercial necessity. Fraud losses in the early 1990s were unsustainable; something had to be done.

Progress was made possible by technical standards (the "framework," if you will). Standards ensured chips and the data in them complied to specifications and functioned with point-of-sale terminal infrastructure. Meanwhile, the payment messages transmitted by merchants to acquirers and card schemes had to conform to the standards, too. Interoperability was a complicated achievement consumers take for granted.

You may be starting to see the parallel between where payment cards were a decade ago and where digital signatures are now. A global system won't gain traction and succeed without interoperability and convenience/ease of use.

Consider this maxim that EMV illustrates: Once a mechanism becomes established, subsequent rates of deployment and innovation accelerate. Chip cards were the first new thing in decades, and subsequent evolution of contactless cards has been impressive.

IN THIS CHAPTER

- Defining the properties associated with digital security
- Understanding the basics of encryption
- Moving from encryption to digital signatures
- Using digital certificates to build trust

Chapter 2
Demystifying the Technology

Before delving further into the wonderful world of electronic signatures, it's worth considering what "information security" really is. Digital signatures are all about providing security while using the Internet, but information security is an even wider subject than that. This chapter explores concepts that underpin the security of all such online digital systems, and then explains how those concepts serve as the building blocks for digital signatures.

Security Is A PAIN

Ah, information security! Hackers, malware, bad guys, black hats, the dark web — the list of concerns gets longer every day. What a scary subject, or so the media would have people believe. But take it from experts: Information security doesn't have to be so complicated. It can be boiled down to a few handy principles.

TIP

Suffice it to say that security is A PAIN. Right, you say, who doesn't know that? No, what we're talking about is an acronym: A-P-A-I-N. The acronym will help you remember the components that are essential to information security. Digital security is a combination of any or all of the following:

Availability

The most "secure" computer in the world would be one encased in concrete at the bottom of the Hudson River. If all your assets were on that hard drive, you could rest assured that they would forever stay private.

A facetious example, of course, but it's an extremely important point. That particular computer is highly secure because it is, in IT terminology, unavailable (or in British slang, it's "knackered"). Realistically speaking, however, just how useful would a computer be if it were sunk a hundred feet underwater off the shore of Manhattan? Not very. Everyone wants systems that are secure but available, often 24/7 on demand.

REMEMBER

It can't be stressed enough that "availability" is integral to real-world security. When someone designs a digital signature solution, the point is to end up with a system that's bullet-proof, easily maintainable, but also continuously in "high availability" mode.

Privacy

The good thing about this A PAIN mnemonic is that it's all fairly obvious once you know what the letters stand for. The P is no exception.

Everyone knows what privacy means and why it's so important. In the context of digital security, privacy usually goes hand-in-hand with encryption. Encrypt something, and it'll provide pretty good privacy.

You don't always need that level of privacy, though. Digital signatures often need to be public because they should be publicly verified. This is the case for such things as digitally signed legal documents, including mortgages. It's good to know when you need privacy, and when you don't.

Authentication

This is the big one! It's also unquestionably the hardest to achieve, and the most important one to never forget. You can encrypt all your documents and all the other files on your laptop, yet it'll be worthless unless you have a strong way of allowing the right people to decrypt the files.

There's a big industry out there concerned solely with ensuring that only the right people get access to the right resources. For now, just remember that privacy and authentication are inseparable.

Integrity

Think about it for a minute. A "transaction" in the broadest sense is any action in which the state of the system changes — that could be money moving from your account to someone else's, or perhaps a document changing from unsigned to signed. In any transaction, you always should ask yourself, "How do I *know* this is the right text or the right account number?" In other words, could someone have tampered with it?

REMEMBER

Happily, the digital world offers several techniques that can be used to ensure this integrity, guaranteeing it to an extremely high level of confidence. One technique is known as "hashing," and there will be more detail on that elsewhere in the book.

Just to muddy the waters, note that some consider the I in this acronym to also represent identity, because that's a necessary part of authentication. You have to know who someone is before you can authorize that person. But, others would argue that identity goes without saying, because you can't have authentication without identification. For the sake of simplicity (and to prevent having to spell A PAIN with two I's), the discussion here focuses on just one of those I's.

Non-repudiation

Say that you receive a digitally signed document and, for good reasons, you know with certainty that it was signed by the person it claims to have been signed by. You'd have an extremely strong case if you had to prove the signature was genuine in a court of law, and that means what you have is a document that is not repudiable.

Put another way, non-repudiation means you'll be able to prove something happened (it cannot be repudiated). It's no coincidence that this property is the logical byproduct of the properties that preceded it — if the document has strong authentication and integrity, that's the basis for non-repudiation.


REMEMBER

Privacy isn't a necessary part of non-repudiation, but it's certainly never detrimental. Meanwhile, the high-availability of a system also contributes to the credibility of the signature (a system with zero downtime is much less likely to have been tampered with).

Putting it all together

With any digital system for which you're responsible, you should ensure you have these aspects of digital security well covered. If you do, there isn't much that ought to keep you awake at night. Now, keep reading to find out how to make it all happen.

The Science of Encryption

Encryption, also known as scrambling, is the science of hiding information (some might say it's actually an art). But this isn't hiding in the traditional sense, such as sticking cash under your mattress. Encryption is hiding information in plain sight. It sounds magical, doesn't it? Some of it almost is.

How can this be done? Well, consider this scenario. You're gathering supplies to redecorate a room in your house but you want to keep the color a secret. The paint containers are unlabeled, but all it takes is someone to open the lid and your secret is out! How can you make sure no one finds out what color paint is in the can? Here's a thought: Get some black paint and mix it in.

Here's where the magic comes into play, so you might have to suspend your disbelief a bit. Once it's just you in the room, you extract the black paint and, voilà, you've recovered the original color. It was there all along, hidden in plain sight, but no one could see it because of all the black paint mixed in.

Digital encryption works very much like this made-up scenario. It involves mixing random data into your valuable but sensitive information. The real info is still there, hidden in plain sight, and decrypting it is a lot easier than separating black paint that's been mixed into a favorite color.

In practice, the way it works is that clever folks come up with ingenious mathematical methods to mix in the random data (usually through a lot of substitutions and scrambling, also known as *permutations*). The method is called an *algorithm* and the random data is the *key*. Different algorithms use keys of different lengths but they all follow the same general concept. Common algorithms go by the names of Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Guess which one came first, and which you should probably now use!

Here's an overly simplified example. Say your message is "hello" and "stendec" is your random key. You might end up with something like "stenodecldecldecedechsten." Now let's parse it a bit, to emphasize where in that mess you can find the actual message: "sten**O**dec**L**dec**L**dec**E**dec**H**sten." Notice that the garbled message actually retains all the information needed to recover the original message (the *plaintext*).

The ingenuity of modern cryptographic algorithms, such as AES, is that they mix in the randomness so well that you can never tell where it is (just like mixing paint). Thus, you can never tell where or what the message is.

An aside for students of synonyms: Another word for randomness is *entropy*. The more randomness your algorithm creates, the more entropy. Algorithms such as AES can use up to 256 bits of entropy (2^{256}, which is a huge number). That's enough to ensure that any amount of data gets turned into gibberish.

DIGITAL SECURITY AND THE PHYSICAL WORLD

Even in the digital world, there's an extremely strong dependency on the physical world to achieve security. There really can't be any security in digital systems without a completely enclosing layer of physical security.

The most expensive and secure digital solutions still must be housed inside very expensive, secure data centers. What's more, the processor chips themselves often need to be covered in epoxy goo to further physically protect them from tampering.

Encryption and Digital Signatures

There's a memorable scene in Disney's *The Little Mermaid* in which the whole premise of the film is laid out. Ursula, the sea sorceress, has the mermaid Princess Ariel under a spell that turns out to be an unbreakable contract — Ursula transforms her into a human in return for Ariel's voice. When Ariel's dad, King Triton, finds out about this, he is none too pleased and immediately tries to destroy the contract with his mer-powers and his trusty trident. But, alas, the power of the contract prevails, and shenanigans and great songs ensue. The point, of course, is that *somehow* the contract was rendered unbreakable.

It's not a fantasy to claim that digital signatures have a very similar kind of power. The difference is that, instead of the power of magic, digital signatures are based on the power of mathematics and public-key cryptography.

Public-key cryptography

Books have been written on this topic, books that are much bigger than the one in your hands now. It's a very deep subject. The good thing is, an understanding of the properties of public-key cryptography will suffice, and that's a whole lot easier than reading a dense text.

Symmetric encryption is the most familiar kind of cryptography. Simply put, this happens if you want to chat in private with someone and you share a key with your confidant. This works just fine until you need to chat with all your many social media contacts. This method doesn't scale well, because each friend needs to have a different key.

REMEMBER

What if, on the other hand, you needed only one key, no matter whom you wanted to privately chat with? What if you had your own, unique key? Well, this is exactly the problem solved by *public-key cryptography*, also known as *asymmetric encryption.* Instead of having a key associated with a relationship — that would be you and your confidant — you have your own key (actually a pair of keys: one public, one private). Your friend can now encrypt with *your* public key, and only you can decrypt it!

This wonderful technology results from the magic of a particular set of "one-way" functions, also known as *algorithms.* These

algorithms give a scrambled output (encrypted text) that can't be reversed unless you have the private key.

And here comes the icing on the cake — what if *you* encrypt using your own private key? Because your public key is already out there, this means literally anyone can decrypt it. So what on earth is the point of that?

Remember that the keys are unique. Only you are able to encrypt something with your private key. If someone decrypts this message using your public key, the ability to do so is evidence that you are the one who encrypted the document.

REMEMBER

Now replace the word "encrypted" with the word "signed." Drum roll, please . . . it's a digital signature!

Before moving further along in this discussion, it's worth recapping the nature of a non-digital signature (otherwise known as a *signature*). A signature is physical and provides strong evidence that a person intended to sign a specific text. The signature indicates that the person performed a contingent action (signing) representing the intention to commit to the thing being signed.

A digital signature has exactly the same properties for digital assets or documents. It achieves this, of course, through a different mechanism — public-key encryption.

All the minute details of encryption and public-key cryptography aren't really necessary to gain an understanding of digital signatures. The important point is that public-key cryptography has all the properties you need:

- Unique identification (with public keys, each individual gets his or her own key, and there is never a need to share the secret key).
- Proof that a particular document was signed (encrypted) and not tampered with. This is achieved with the power of document hashes (see the sidebar on this topic).

REMEMBER

To sum it up, digital signatures are an exploitation of the properties of public-key cryptography to create a practical analogue of physical signatures that will satisfy all the necessary criteria. But wait, there's more! Thanks to the tamper-evident nature of digital signatures, you can have even more confidence in them than traditional signatures. After all, how would you ever really know if a physical document has not been tampered with unless you employ expensive experts to verify that everything is okay?

HASHING THE MESSAGE

Imagine all the digital documents that ever existed or ever will exist. That's a ridiculously large number, isn't it? Now imagine all the documents that could *ever* exist. That's not even an imaginable number; that is infinity!

Hashing is a process (or "function") that copes with these astronomical numbers. It has these properties:

- As input, it can take in any possible document (or any digital data).
- As output, it produces a document fingerprint (a fixed-length, unique identifier, such as a car license plate number).

A *secure* hash has two more properties:

- It must give a unique fingerprint for every single document.
- It must be unfeasible to regenerate the document from the hash.

Here's a fun quiz: Can you identify which specific aspect of security is covered in these two properties of a secure hash? Remember: Security is A PAIN. Look for the answer at the end of this chapter.

The benefit of hashing is that the fixed output is much smaller than any useful document and, because it's unique to your document, you only ever need to sign the hash data. This will still count as signing the document.

What's the catch? There's a quite big one — the uncertainty of knowing whether the hash is really unique for all possible documents. The solution is to use a bigger hash. The standard hash algorithm is now SHA-256. This means every atom in the universe could have its own unique hash value. Seems like we'll be safe for a little while longer.

What is being signed?

REMEMBER

By this point, it's clear that the functions involved are digital processes (or algorithms) all based on clever mathematics. Does it really matter what is being signed? Not to the algorithm. In other words, you can use this technique to sign anything that is digital — text, images, computer programs, you name it.

But, of course, the nature of the thing we are signing matters to us, so it's worthwhile to categorize data types in the following way:

- **Documents:** These contain human-readable text that has assertions or commitments (such as in a contract).
- **Transaction data:** This involves human-readable text that has *state-changing information* (such as, "pay $1,000 from my account to account X").
- **Binary data:** This is machine-readable data that is signed to attest the *origin of the data* (or the possible ownership of the data).


TIP

The digital signature mechanism does not change to any significant extent based in the type of thing being signed. On the other hand, the front-end interface and the workflow must be designed around what is being signed, depending on whether or not a human is involved. It is possible to demarcate what can be signed and by whom through the use of digital certificates — more on these shortly!

It's a matter of trust

You've almost completed the journey through the technical jargon and mysteries of cryptography as used for digital signatures. There's one last hurdle to deal with, as suggested in the sidebar about indirection.

What's the final problem we have indirected to? The authenticity of someone's public key. What techniques are there to attest to the authenticity of a public key?

The answer breaks down into various categories:

- **Ad hoc:** You could rely on telling people what the key is over the telephone so they would know the key came from you (this could work, but no one ever does this).
- **Peer-to-peer or web of trust:** All participants in the communication trust each other.
- **Hierarchical or trusted third party:** Two mutually distrusting parties agree to trust a central party or, more likely, a *trusted service provider*.

THE POWER OF INDIRECTION

Unless you live in an ultra-safe and polite place like Canada, at some point you'll be concerned about the lock on your door. Why? Because you have *indirected* the problem of securing your house to the lock and the key.

The very wise British computer scientist David Wheeler once said, "All problems in computer science can be solved by another level of indirection." We see this principle admirably demonstrated in cryptography. You start with a whole load of files you want to be kept private (encrypted) so you encrypt them with an algorithm (AES, for example). You've just indirected the problem. You're no longer keeping the document safe, but rather keeping the key safe.

But remember A PAIN? The key needs to be available, secret, its use needs to be authenticated, and it must not have been tampered with (non-repudiation does not apply).

This concept has held through most of human history, but in the 1970s there was a world-changing breakthrough with the invention of public-key cryptography. This breakthrough eliminated one necessary property: the need for secrecy of all the keys. By having two keys to do the job through asymmetric cryptography, one key could be entirely public without any compromise of security.

But always bear in mind two things:

- The other key (called, sensibly enough, the *private* key) must still be kept secret.
- The public key must still be authenticated (and not tampered with).

That last option should sound familiar, because it's the scheme used most often. For example, secure websites use the secure HTTP protocol TLS, and card payment infrastructures rely on EMV. The peer-to-peer model has been exploited in environments such as PGP (and its open-source cousin, GnuPG) and SSH.

A word on blockchains

Blockchain technology and its relationship to public-key cryptography is an interesting and hot topic. Some blockchain applications such as crypto currencies and smart contracts are *consumers* of public-key cryptography because they depend on digital signatures

to ensure the unique identification of transactions. Critically, however, these transactions can still retain anonymity, because identity is based on anonymous numbers.

But a blockchain is a good model for also *supporting* public-key cryptography because it is an ideal peer-to-peer, decentralized network.

The Need for Digital Certificates

How does the certificate differ from the signature? A digital certificate is primarily concerned with only one thing: the pedigree of the public key. Where did this key come from, who owns it, and what will it be used for?

A signature is dependent on only the keys and the document. If you're already satisfied about the origin of the public key, you don't need a certificate (this is the rare case of the ad-hoc method). But just about no one uses this scheme, so it is safe to assume a certificate is always needed.

So, a digital certificate is a digital signature of:

- A public key
- The identity of the entity to which the key belongs
- The restriction on what the corresponding private key can sign (only emails or only code, for example)

This certificate is signed by the private key of an entity that claims to be able to be trusted.

REMEMBER

Sometimes there's a whole chain of these certificates and signatures, from the lowest public key through intermediate bodies right up to what is known as the *root of trust* (a government or root certificate authority). This situation is seen especially in the *hierarchical trust model.* Once you get to the end of this chain, you can bet that the private keys of these bodies are kept extremely secure!

This leads to the last level of indirection. When it comes to digital security, the absolute final stage is deciding if you trust the certificate-issuing mechanism. That may be a trusted service provider or perhaps some decentralized group of people.

X509 DIGITAL CERTIFICATES

Connect to any website over the secure HTTP protocol (HTTPS) and the certificate will be in the most common format: x509.

There isn't anything special about this format, really. It does the job, which is to say that it attests to anything you could ever want to know about the public key (in the case of your web browsing, the key that was used to set up the secure channel between your browser and the web server). That includes the domain to which the key is registered (its identity), the key properties such as size and algorithm used (of course), and the fact that it is only supposed to be used in the context of a secure website (and not to, for example, sign documents).

x509 is a standard that defines certain other relevant entities in this world, such as the format of a list of bad (revoked) certificates. But, by and large, the name is firmly associated with the certificate.

REMEMBER

Some three decades of commercial experience reveals that the trusted third-party scheme of issuing certificates underpins most public-key infrastructure (PKI) today. The institutions at the center of this are called *certificate authorities.* Trusted third parties will either use the generalized, catch-all certificate format defined in the specification x509 (see the sidebar for more on this topic) or will use certificates particular to their application (such as EMV for card payments).

And one last thing: That question about hash a few pages ago. The "secure" in "secure hash algorithm" refers to protection of *integrity*. That's because any change to a document produces a different hash. In that way, tampering can (potentially and theoretically) be detected.

IN THIS CHAPTER

- Exploring the business models
- Examining different signature formats
- Building architectural frameworks
- Signing what you see
- Spelling out the case for remote solutions
- Creating regulations that make it all work

Chapter 3
A World of Possibilities

This chapter explores where the business-to-business (B2B) and business-to-consumer (B2C) models for digital signatures are right now, and how far they've come. It spells out signature formats and technical frameworks, as well as the regulatory standards that are allowing digital signatures to gain the legal authority and level of trust formerly reserved for pen and ink.

Where the Business Models Stand Now

It certainly makes sense that the market for digital signatures is exploding. If you can offer an end-to-end digital service with legally binding user consent, the result is lower costs, increased security, and greater confidence in transactions. Digitalization enables paperless processes, and in making that happen, it reduces emissions and supports sustainable business growth. In Europe, the Electronic Identification, Authentication and Trust Services (eIDAS) regulatory framework now offers a realistic promise that digital signatures can be accepted throughout the

European Union, which means new freedom for users and transparency for service providers.

This is part of the whole quest, the driving aspiration for those promoting the use of digital signatures, especially in Europe. But why stop with Europe? The endgame has to be global, just like the Internet itself.

Consider how much the spread of the Internet would have been hampered by independent standards emerging just as things were getting going. And consider the progress of EMV in the card payment world over the past 20 years. It caught on like wildfire in many countries, while it's slowly (but surely) winning the battle in others.

REMEMBER

The B2C market sector will see major benefits, from cost reduction to much faster, entirely electronic, transaction cycles. For some perspective on how things might transpire, consider the growth in online and mobile banking over the last decade or so.

Online banking services started off relatively slowly, compared with the more recent growth in mobile platforms. But take-up for straightforward banking transactions has been so strong in recent years that traditional bricks-and-mortar bank branches are declining quickly. Consumers are willing to transact online at scale if it provides convenience. Whether they like it, or simply feel they have no choice, those are different questions.

Providing traditional physical infrastructure for banking services has shifted focus toward developing flexible online and mobile platforms, where infrastructure costs are much lower and the consumer provides the contact device/endpoint. Digital signature technology is now at the same tipping point. Whether it be in the B2C or B2B markets, businesses, citizens, and consumers all have the contact device/endpoint infrastructure.

The hard work has been done by security product vendors and various other entities over the last 30 to 40 years, ensuring that you can concentrate on the business questions when designing your digital signature service. To see how the customer's journey improves when you deploy a digital signature system, see Figure 3-1.

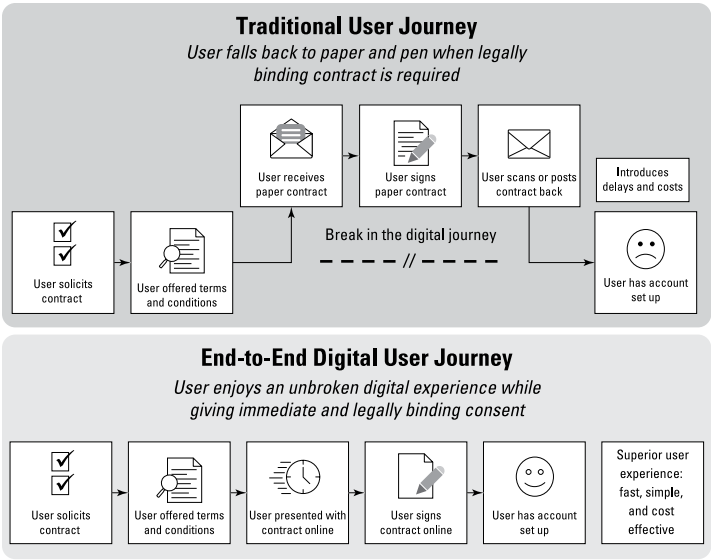

FIGURE 3-1: Improving the customer journey — digitally.

Defining Digital Signature Formats

It's worth now delving into the technologies that are underpinning these deployments as well as the regulations that give digital signatures meaning in the real world.

One of the big questions you'll face as you plan a deployment is, what will happen to your signed data? Will any applications need to use the data? Which applications? Will the data need to be timestamped, archived, or otherwise stored?

REMEMBER

Answers to these questions determine the format. Once data is signed, it's effectively sealed so that it can't be changed after signing, without detection. So, targeting a certain format is very important, right from the start.

The PAdES format

PDF readers are good examples of applications that use digital signatures in a specific format. The format that has been defined is PDF Advanced Electronic Signatures (PAdES). It's a set of standards created to support European requirements for electronic signatures.

One important benefit of PAdES is that electronically signed documents can remain valid for long periods of time, even if underlying cryptographic algorithms are broken. It's vital to always be able to validate the document to confirm that the signature was valid at the time it was signed — in spite of any technological and other advances. This is a concept known as *long-term validation,* and there's more on the topic in Chapter 5. PAdES also caters to bulk signing. In one authorized session, multiple files can be digitally signed.

PAdES, when used for signing PDF documents, is specific to an application. That potentially can cover any case for human-readable information that it need not be processed by a computer (just like a document signed in the traditional way).

Thus, it's very useful, but it still leaves a large gap for other use-cases. After all, digital signatures also apply to human-readable information that *is* intended to be further processed by an application — for example, high-value financial transactions.

The XAdES and CAdES formats

Beyond human-readable information, signatures should also cover the case of *binary* information (such as an executable or .exe file), a code library (or DLL), or even a media file (such as an .mp3, .jpg, and so on). Signing binary information predominantly serves the purpose of identifying the source, for copyright or security reasons. These two formats deal with this category. They're general-purpose formats that can deal with any structure of information.

REMEMBER

XML Advanced Electronic Signatures (XAdES) is a standard that defines the envelope in which data and its associated signature can be encapsulated, making it suitable for electronic signatures. The standards bodies — the World Wide Web consortium (W3C) and the European Telecommunications Standards Institute (ETSI) — maintain and update XAdES together. ETSI is on a par with the National Institute of Standards and Technology in the United States.

While XML-DSig is a general framework for digitally signing documents, XAdES specifies precise profiles of XML-DSig, making it compliant with the European eIDAS regulation (more on that later).

TECHNICAL STUFF

The data within an XAdES "package" (a self-consistent unit of data + signature) is intended to be human-readable, and is expressed with XML tags.

This XML data structure includes all the necessary information to identify the signatory, such as the International Bank Account Number (IBAN) in the block of XML data, when used for a banking transaction.

With the included signature of all the data, plus the certificate that attests to the authenticity of the public key used, the banking system will decide that the details are all sufficiently verifiable, trusting it and performing the high-value transaction. Ideally, the bank can consider that such a transaction will not be successfully repudiated.

As with PAdES, documents signed electronically using XAdES can remain valid for long periods, even if underlying cryptographic algorithms are broken.

REMEMBER

CMS Advanced Electronic Signatures (CAdES) shares almost all aspects in common with XAdES, in terms of its security properties and how it is maintained. There's one big difference — it's intended to be deployed only for signing binary data.

Together, the PAdES, XAdES, and CAdES frameworks adequately cover all use cases: any human-readable document, any human-readable transaction, and any arbitrary binary (machine-readable) data.

Building the Architectural Frameworks

In general, there are two methods for generating secure digital signatures:

- Local signing using smartcards, in which users must retain and protect their private signing key.
- Remote signing technology, in which the users' private signing keys are stored and protected in a central location but can be accessed remotely by the user.

Smartcards or chip cards, used for providing digital signatures for electronic commerce, never caught on in any significant volume because few smart card readers exist. Such solutions restrict usability and are prohibitively expensive.


REMEMBER

For those reasons, it makes more sense to focus attention on the second digital signing approach — remote signing servers or "signatures in the cloud," introduced by Cryptomathic in 2001, long before cloud solutions became fashionable. This approach has been a success in many countries such as Denmark, Luxembourg, Norway, and Switzerland, and the concept is catching on outside Europe as well. It's an extremely cost-efficient solution.

But you need to start with the applications that make it most attractive to end-users. Consider how attractive e-banking and Internet shopping have become. Think of all the letters you get throughout the year from public authorities, having to do with taxes, registration for voting, pensions, and the like. Now you can start to get a picture of how significant it is to digitize all this activity and make it easy!


REMEMBER

So, what's needed? There's one and only one way to secure data on the Internet: by means of cryptography. And for this, you need keys — private keys for digital signatures and decryption, and corresponding public keys for signature verification and encryption. Of course, you also need:

- Access to your apps using your cryptographic keys
- Secure storage of the keys
- Secure generation of signatures

Put it all together, and you'll see that you need cryptography, and also systems that meet the many other challenges presented, such as answering the rather important question of, how do you know if you are signing the right thing?

Are You Signing What You See?

You may be familiar with the acronym WYSIWYG, short for "what you see is what you get." In 1998, a twist on that concept emerged. Cryptomathic's Peter Landrock and Torben Pedersen coined a

variation in the *Information Security Technical Report,* in an article titled "WYSIWYS? What You See is What You Sign?"

WARNING

Here's the point. When you read something off your screen and you want to commit to it — just as you would once you've finished reading through a paper document — how do you know what you just read is really is the message to which you are committing? This really is a challenge unless you have a completely trusted graphical user interface — and you don't, because GUI interfaces still have security holes.

How about storing the private key on a chip card? That doesn't in any way address this challenge. The only way to deal with this case is to use two independent channels, because it is very unlikely and costly for both to be successfully attacked at the same time.

REMEMBER

One good, though not recent, realization of WYSIWYS is the Chip Authentication Program, developed by MasterCard and later adopted by Visa as Dynamic Passcode Authentication. It requires a stand-alone card reader and an EMV chip card.

TECHNICAL STUFF

With this technology, once the user has provided the details of a payment on, for example, a workstation, the user is asked to insert the debit or credit card into the card reader, type the PIN, and press the Sign button. The user is then required to key in the amount to be paid and the account of the payee. The chip card generates a digital fingerprint that ensures the transaction is unique, displaying it in the reader. The user subsequently keys this in, together with the full transaction, on the workstation.

The cryptography behind this process is a symmetric encryption system, with a key shared between the payment card and the bank's back end. Thus, WYSIWYS can be achieved using a combination of symmetric cryptographic techniques and tamper-resistant hardware.

Signature schemes based on public key techniques are also particularly useful in electronic commerce, where many independent parties communicate with other independent parties. So, before one can even think of providing WYSIWYS in e-commerce, it's necessary to establish a *public-key infrastructure (PKI).* Each user must be registered and have sole control over the usage of his or her corresponding private key.

Why Remote Signature Server Solutions Are Preferable

With a central signature server for remote signing — you might call it "signatures in the cloud" — the challenges are:

1. The users are properly authenticated before they can sign a message.
2. Only the owner of a particular private key can initiate the signature calculation.
3. WYSIWYS.

To protect the signing keys, each server is supported by tamper-resistant hardware boxes, so-called *hardware security modules* (HSMs), and all secure calculations and verifications are carried out entirely by and in an HSM. This is very much like how payment card transactions are authorized by banks. The following sections summarize how remote signature solutions can solve the challenges and provide benefits beyond local signing mechanisms.

PKI becomes invisible

The concept of public-key infrastructure hasn't always been well received. The experiences of various PKI pilots by the end of the previous millennium were not always positive, and some banks and companies declared PKI to be dead and useless. This conclusion, of course, has turned out to be completely wrong.

REMEMBER

The new generation of debit and credit chip card (EMV) technology is based entirely on PKI, and it's a great success. Why? Because the PKI provided is invisible to the user. This is also the case with central signing. From the user's perspective, the experience is a workflow that's just like logging into any online service. That's indirection, working for you!

This approach enables significant simplification, and it removes the shortcomings of a traditional PKI solution, in which everybody may communicate securely with everybody else.

First of all, once a user is properly identified and registered, his or her private key pair is generated by the signature server — and never leaves it — and the signature server can have a certificate issued at the certificate authority (CA). The CA *only* issues such certificates for signature servers that are associated and adhere to the same kind of solution and security level. In that way, all applications for which this infrastructure is used will in principle be able to recognize if a signature received from another user has been generated on a secure server, as opposed to a chip card.

Certificate expiration and revocation are no longer issues

With the central signing server approach, revocation becomes a non-issue, except for a very short clearing period. Indeed, with this approach, the millisecond a certificate is revoked by the CA, the CA informs the central signature server, so requests from the user to sign with his private key are no longer honored.

This means there's no longer a need for blacklists, if the CA used in conjunction with a central signing solution issues certificates only on public keys for which the private key is stored with an authorized central signature server. Indeed, when you receive a digital signature generated by the central signature server, you can be certain that the private key used to generate it must have been valid at the time the signature was generated!

The end of blacklists

One of the major discrepancies of most PKI solutions involves the handling of revocation and blacklists, which indicate whose certificates are no longer valid. A big problem with blacklists is that pretty much as soon as they're generated and distributed, they become obsolete and out of date.


REMEMBER

That's why it's advantageous, in remote signing, to use a CA that issues certificates only on public keys for which the private keys are stored within an authorized central signature solution. You no longer need blacklists!

Independent timestamping is no longer required

Independent timestamping is required in a traditional PKI solution (every user has a private key on a smartcard and signing takes places "locally") because you either need to send all received signatures to an independent third party for timestamping, which is the most common approach, or have other means of proving when the signature was received. Otherwise, it's too easy to compromise this process because it is performed on an untrusted environment. No such restriction applies to remote signing because the entire environment where signing takes places can be trusted.

Remote signing works on the latest smartphones and tablets

Remote signing can securely exploit the technology on today's smartphones and tablets, and encompass all the required functionality for authentication. That's been possible since 2003, even when we only had Java-based feature phones. It doesn't need specialized tokens for local signing or computation-heavy libraries for the signing algorithm. In the jargon of security vendors, it is a "zero footprint" solution.

It is now possible to reuse existing 2FA deployments, so users don't need additional hardware or software to sign. They can sign with any device that has an Internet browser or app. Not having to deploy dedicated signing equipment also makes it very cost-effective for large-scale signing services.

What it all means

Remote, central, or cloud signature servers are superior. They're the only architecture that fits all current and future requirements, especially regarding maintenance and control of the authentication end. This technology is the most likely enabler of large scale e-government and electronic commerce solutions. It's as safe as or safer than the old-fashioned chip card approach, it enables WYSIWYS, and, last but not least, it makes the underlying PKI invisible to the end-user because it can reuse existing authentication mechanisms. In addition, it removes most burdens of revocation, such as blacklists.

Europe Pioneers the Regulatory Framework

In so many cases, the law falls well behind technological advancements — just think about the issue of controlling hate speech on social media. But that isn't the case with this area. The legal framework for electronic signatures was put in place before the industry reached critical mass, leading to widespread adoption of electronic signature applications, especially in Europe.

Back in 1999, the European Union adopted legislation for the legal acceptance of digital signatures with a few conditions. One of these conditions involved the use of a secure signature creation device (SSCD), and the only solution anticipated was a chip card.

In the meantime, it has become clear that central signature server solutions are much more appropriate and practical. There are now nationwide deployments in countries across Europe and the Middle East that are highly successful, with more than 60 percent of all citizens in some countries using these solutions on an almost daily basis. The European Commission has recognized this trend, and the eIDAS regulation now allows for a central signature server as a remote SSCD.

REMEMBER

The Electronic Identification, Authentication and Trust Services (eIDAS) regulation creates a new system for secure electronic interactions across the EU between businesses, citizens, and public authorities. That includes the use of digital signatures.

This regulation applies to electronic identification (eID) schemes for which EU countries notify the European Commission, and it covers trust service providers based in the EU.

So, in the Euro zone, there's a very comprehensive legal framework for the use of digital signatures in business. It seems likely that this will become a model for future developments in digital signature law across the globe.

REMEMBER

The eIDAS regulation officially became law as of July 2016, though at the time this book was being written, some of the technical standards were still in draft format. The standards are mostly controlled by the European Telecommunications Standards

Institute, or ETSI. Cryptomathic, as a security product vendor and a member of the standardization committee, is entirely optimistic that by the middle of 2018, all major technicalities will be defined, and in several cases, in production.

In many ways, eIDAS can be considered on a par with the June 2000 U.S. government e-sign bill, but there are several areas where eIDAS is more comprehensive:

- eIDAS introduces the new concept of digital "sealing," which is when digital signatures are issued on behalf of a legal entity such as a corporation. Appropriate-use cases include signed bills, emails, code, intellectual property, and a nearly endless list of other possibilities.
- eIDAS covers the entire ecosystem of digital signatures (it regulates "trust services," a super-set of certificate authorities).

Here's an example of eIDAS at work: If the validity of a digital signature is challenged, courts are not obliged to accept XAdES-based electronic signatures as evidence unless they're classified as Qualified signatures. For the lower-grade case of Advanced signatures, a judge need not accept the evidence unless there's an individual case made that no part of the procedure was compromised at any point in the chain.

Authentication assurance: The three levels

eIDAS recognizes the challenges that any organization will have before, during, and after deployment of a digital signature solution. One of the major challenges will always be, how do you really know who is signing the document?

REMEMBER

That's where the definition of the three authentication assurance levels is relevant. The levels are *Low*, *Substantial*, and *High.*

If you're renting a vehicle, for example, the digital signature really only needs Low assurance (a password or similar *single-factor* authentication method). When the value goes up, such as a loan for 1,000 Euros, Substantial authentication assurance is warranted. That generally translates into two-factor authentication

(such as a password and a one-time SMS code delivered to your phone).

But digital signatures have the capability of underwriting transactions around the million mark. That's when you'll be glad to have a High assurance level.

High assurance requires stronger techniques than, for example, SMS (which has experienced social-engineering attacks). Techniques such as challenge-response authentication, embedded in a certified hardware token, must be deployed.

These assurance levels also refer to the type of identification required for enrollment of a user. The full details of this method are published in the 2015/1502 act, which supplements the eIDAS regulation.

Signatures: Qualified and Advanced

Signatures and certificates can be classified according to the circumstances under which they were generated. This indicates how the person or business wanting to sign was registered.

REMEMBER

eIDAS defines three categories of electronic signatures: *Basic, Advanced,* and *Qualified.* It isn't really possible to recommend the Basic level for any suitable purpose, as it will have little value in a court if the validity of the signature is challenged. Given that, this book doesn't discuss it further. The higher security classifications of digital signatures are called an *Advanced Electronic Signature* and a *Qualified Electronic Signature.*

REMEMBER

An Advanced Electronic Signature (AdES) means that:

- It is uniquely linked to the signatory.
- It is capable of identifying the signatory.
- Only the signatory has control of the data used for the signature creation.
- The signature becomes invalid if the data associated with the signature has been changed after signing.

This is codified in eIDAS by EU Regulation No. 910/2014 for electronic transactions. You'll find similar restrictions in the June 2000 U.S. government e-sign bill, as well as in Switzerland through the digital signing standard ZertES.

A Qualified Electronic Signature is an Advanced Electronic Signature with a qualified digital certificate, and for which the signature has been generated by a qualified signature creation device. The Qualified certificate is issued by a qualified trust service provider, and it attests to the authenticity of the electronic signature to serve as proof of the identity of the signatory.

REMEMBER

Simply put, a Qualified Electronic Signature (QES) increases the level of security over what an Advanced Electronic Signature provides. Within the EU, a QES is considered by law to be the equivalent of a handwritten signature. There currently is no QES counterpart in the U.S.

A Qualified certificate is a certificate that has been issued with High assurance (this often means a face-to-face interaction or a live video interaction for initial identification purposes).

But creating a QES is more than merely adding a Qualified certificate to an Advanced Electronic Signature. As mentioned, it also requires the use of a qualified signature creation device, and that is a key piece of the puzzle.

REMEMBER

The details get very technical very quickly, but here are the basics. For remote QES, you need:

- A certified hardware security module (HSM)
- Certified signature activation module (SAM), running code on the HSM that ultimately signs the document (under strict authorization of the signatory, of course!)

SAM + HSM = a Qualified signature creation device (QSCD). Check Figure 3-2 to see where the secure hardware fits in.

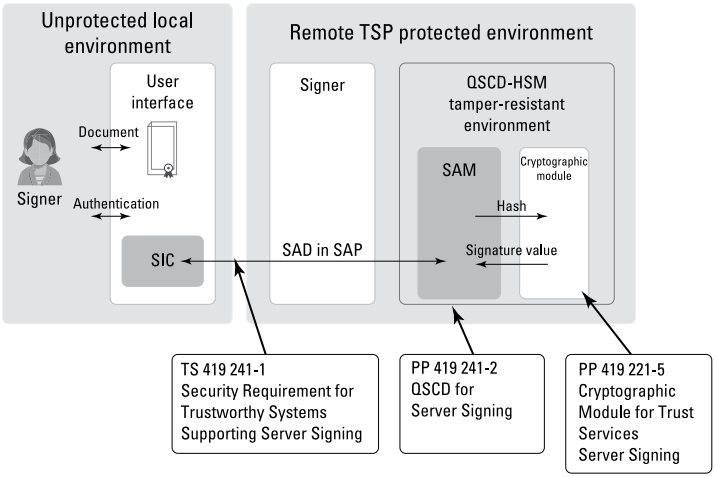

FIGURE 3-2: ETSI standard 419241 (and associated protection profiles) indicating usage of cryptographic hardware (HSM) and secure code (SAM) within the remote environment and the secure channel connected to the signatory UI (SIC).

Digital Signature Law in the U.S.

REMEMBER

Both the United States Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA) have four major requirements for an electronic signature to be recognized as valid under U.S. law. Those requirements are:

- **Intent to sign:** Electronic signatures, like traditional wet ink signatures, are valid only if each party intended to sign.
- **Consent to do business electronically:** The parties to the transaction must consent to do business electronically.
- **Association of signature with the record:** The system used to capture the transaction must keep an accurate log of the signature process.
- **Record retention:** This requires that electronic signature records be storable in an archive, and reproducible for viewing by any entitled party.

Both federal laws stipulate the following:

- No contract, signature, or record shall be denied legal effect solely because it is in electronic form.
- A contract relating to a transaction cannot be denied legal effect solely because an electronic signature or record was used in its formation.

These two acts have simplified the legal framework for using electronic records and electronic signatures in commerce.

REMEMBER

If you compare U.S. digital signature law with eIDAS, there's no doubt that eIDAS is much more comprehensive. That's because eIDAS deals not just with the requirements for sole-ownership type signatures but also the newer model of "sealing," and also the entire ecosystem that supports the basis of trust for digital signatures.

REMEMBER

The bottom line is, the scope of eIDAS is enormous, covering the entire digital ecosystem — you could call that a maximalist approach. U.S. law, on the other hand, takes a minimalist approach to support the technology and industry. And because U.S. law relies more on case law to establish the final meaning, it's no surprise that the first few smatterings of cases dealing with the legality of "dig sig" law are coming from the U.S., not the EU.

Laws in Other Jurisdictions

Switzerland follows an extremely similar legal framework to eIDAS *and* there are several good examples of each kind of digital signature solution. The framework is called ZertES, and several digital signature solutions exist in Switzerland, audited and certified up to Qualified level, just like eIDAS.

ZertES shares many of the characteristics of eIDAS, except:

- In order to achieve Qualified status, it requires digital signatures to include qualified timestamps.
- Since January 1, 2017, it has been fully specified to state that central-signing solutions can be audited for certification up to Qualified status, achieving the highest legal probity.

IN THIS CHAPTER

- Owning the digital strategy
- Seeking assistance
- Asking the right questions
- Exploring the commercial considerations

Chapter 4
Your Deployment Strategy

This book recommends and implies that your organization must fully consider all the pertinent technical, procedural, and regulatory requirements both now and in future. You'll probably read that and say, "Yeah, right, like we're really going to be able to predict the future!"

You may not have a crystal ball, but you can at least make an informed guess about where things are headed. It's important to try, and there are approaches that can ease your digital journey. This chapter explores how you can obtain help in deploying digital signatures, points out questions you'll need to answer when choosing assistance, and discusses the commercial considerations that accompany the use of digital signatures.

Digital Strategy Is Yours to Own

Your organization might be in the midst of one or more of the following scenarios:

- You're new to the world of digital signatures.
- You have a business/IT project in development or enhancement, or maybe several projects simultaneously.

- You've implemented one or more digital signature initiatives, and you're now wishing to expand usage.


REMEMBER

Wherever your organization is on that menu of potential scenarios, one thing is certain. You must own the management and ongoing development of this element of your digital strategy. You can't let some initial IT project, and its IT developers, determine how your digital signatures will be used and managed. That's the organization's responsibility, and it should not be abdicated. The ongoing management and development of your digital signature usage will be required long after any project is completed.

Getting Help

If you've read the earlier chapters, you will recall that digital signature technology has been around for 40 years. Practical implementations at scale, however, have only been possible much more recently.


REMEMBER

There's a distinct benefit that comes from this long development and gestation period. In some cases of technology adoption, even the experts don't have all that many years of experience because the technology is so new. In this case, though, there are companies with long-term involvement and a lot of experience, and your organization can benefit from that expertise.


TIP

Cryptomathic is one such organization. It's been involved in the development of digital signature technology components and their associated technical standards for more than two decades. The company's philosophy is to work in partnership with customers, over years, anticipating capabilities that will be needed and reflecting them into products for immediate and future use.

Here are some of the factors to consider and evaluate when you're seeking help from vendors and consultancies.

- **Digital signatures aren't just about technology.** Your potential supplier needs high levels of actual experience in business integration and management activities, too.
- **You *will* need help.** Yes, it's theoretically possible to proceed with a DIY mentality, but it simply isn't a practical or economic proposition.

- **You'll probably need to buy certain technology components or pay for them on a usage basis.**
- **It's vital to validate the software products you are considering to ensure they are soundly architected, designed, and developed.** They should contain all required feature and function sets, adhere to recognized industry technical standards, and suit your organization's current and future IT deployment models. They should also have credible development and enhancement plans.
- **Hardware products must comply with all technical regulations and meet all technical standards — assume a global reach for your business.** Hardware should also have defined product development paths.
- **Digital signature technology must be integrated with your own IT applications.** Count on the need for some technical customization for every IT system using digital signatures.
- **Be sure to think of the big picture.** Does your potential supplier offer you an attractive and seamless digital signing experience? Ponder and test this.

Checklists and Pointers to Consider

The checklist headings and pointers that follow are intended for you to populate with your own more detailed and pertinent questions. What relative weighting should be assigned to each? That's a matter for your management judgment at the time.

Note that these headings are not in any particular order of priority. You may want to consider applying checklists on a per-project basis, and also on an overall organizational basis. If you do, you'll likely find that checklist contents and weightings will be different for the organization compared to project.

REMEMBER

Also note that many of the checklist headings and their typical considerations interrelate. They often conflict and create tensions with each other, and organizational expectations can often be overly optimistic (that's your "want my cake and eat it, too" scenario). Your choice of a technical partner for your initial foray into the world of digital signature technology is an important, if not crucial, consideration.

Your business strategy

- Are you doing this to establish leadership in a given area, or are you following others (including your competitors)?
- Do you have clear ideas of volumes required and the duration of the usefulness of the digital signature produced to your organization and recipients?
- What are the business drivers? Improve the offer? Lower the cost of doing business? Improve speed of doing business?
- What is current stance (and likely future stance) with regard to the provision of your IT services? Potential answers include being in-house, run by third-party processors, cloud-provisioned (private and/or public), something else, or a hybrid of some of these options.

Commercial factors/influences

- Does your organization cost initiatives on a development/project basis? Do you consider new or incremental ongoing operational costs separately?
- When involved in development projects, do you identify new services that may or will be required, and existing services that may be changed or even superseded? You'll need to set out your organization's criteria to make this assessment.
- Set up your internal assessment methods within your initial development projects to confirm how your digital signature technology will be provided, operated, and resourced within your organization. And do this prior to implementation!
- Set up mechanisms to review your digital signature technology provisioning on a regular basis. Initially, this is likely to be biannual, moving toward an annual review. This matter is organization-specific, depending largely on the rate of take-up and the importance of the topic to the organization in terms of security and business strategy.

TIP

User experience

- What confidence can end-users be given that they are consenting to the transaction they are presented with?

What are the protections from spoofing, man-in-the-middle, and so on?

- How much freedom will be given to the choice of device used (desktop or mobile)?
- Will evolutions or rapid changes in the user experience be required?

Security

- How strong is the business application's system design with regard to protecting against tampering and subversion of documents and processes?
- Does the system make use of trusted hardware (HSMs) to protect vital cryptographic material and sensitive processes?
- What assurances are built into the development and procurement processes for systems and services initiatives using digital signature technology? Will these be applied consistently to all such initiatives the organization is using? Will these be reviewed and upgraded regularly in response to usage within the organization as well as advances in digital signature technology and compliance requirements?

Legal admissibility

- What promises are given regarding the strength of signature in a court of law?
- For the European market, do you want your system to offer fully Qualified Electronic Signatures and compliance to eIDAS or similar regulations, for example, ZertES?
- What quality of audit materials will be provided to prove a transaction took place?

Integration effort


REMEMBER

- How well will the digital signature technology integrate with existing applications and processes? Consider the viewpoints of development, downstream service management, and enhancement.

Scalability/extensibility/operability

- Can the solution be scaled to meet the needs of the business?
- Within your organization, are there different deployment models available to address different business priorities, such as hosted versus as-a-service models?
- Once you have implemented business services with digital signature capabilities, how will you be life-cycle managing and enhancing this initial service?

Reputation and experience

- Does the vendor or partner you use in provisioning certain technical components of your solution have high-quality references available in relevant market sectors?
- Does the vendor or partner have credibility with certifications at the highest reference levels?

Ongoing management

- There will technical and regulatory developments in coming years.
- Your initial digital signature implementation is only the end of the beginning.
- The practical choices you have will be constrained by your earlier choices in response to several of the previous headings.

Now that you've worked your way through those checklists and questions, you can see that it isn't simple. You should be giving as much consideration to what comes next as is realistic. Ignore this at your peril.

REMEMBER

Recognize that organizations are likely to be reengineering certain existing processes when bringing them online. Compared with building new, such reengineering initiatives are often more complex and difficult to accomplish successfully, particularly if significant transition periods are needed.

Frightened yet? That certainly was not the intention. You may not have instant answers to all these questions. The point was to outline the factors that must be considered, and inject a sense of realism.

TIP

Experienced vendors will be able to discuss suitable approaches with you. Working with the right vendor can reduce the size and complexity of your challenges, and keep them within proportions that are manageable and agreed upon. Your goals will be in line with the characteristics you and your vendor agree to. Dissect the project into as much detail as is practical, agree on the constraints, confirm the expectations, and set the timescales.

Commercial Considerations

As spelled out in Chapter 1, organizations are bringing many things online that used to be offline. Enormous savings are possible for governments, companies, individuals, and the environment if we can communicate — and also commit and be held liable — electronically rather than on paper. This is what digital signatures can facilitate.

That's the benefit. What's the cost? How do you obtain a picture of what this is likely to cost? You won't be surprised to learn that the answer isn't straightforward. For one thing, do you want to examine costs from the development/project perspective, or are you also considering the ongoing operational and enhancement costs (the life cycle)?

REMEMBER

There are typically three operating models for supplying digital signature technology services:

- Licensed technology model: The entire solution is installed on premises; typical users are banks and trusted service providers (TSPs) that serve others.
- Hybrid PKI service model.
- Pure TSP model.

Are all these choices on your menu? The answer depends on how much time you have for your initiative.

To consider that, let's assume a green-field start position (how often are you in that position?). The licensed technology model, when used to allow Qualified Electronic Signatures, typically has a time to market of 12 months or so.

How about a hybrid PKI through which a provider such as Cryptomathic delivers some of the services, such as CA, signer, HSMs, and so on, while your organization provides the other aspects, not the least of which is reliable user registration? This model takes six months or more.

The TSP model can take as little as a month. The timeline depends on the capability and offering of the trusted service provider. You won't be able to influence that because you are not assuming any liability.

REMEMBER

Each of these models can be costed, but sensible approaches for estimating development IT initiatives must have tolerance bands applied, based on the factual information and assumptions available. Some of the influences for which you'll need to provide answers are:

- Are you clear on the volumes of digital signatures you require and the peak rates at which you require them?
- What are your likely projections for digital signature usage for each of your business applications, using them for up to two years from initial implementation?
- To what extent are you responsible for the development and maintenance of your existing applications that are or will be employing digital signature technology?
- Do you have the required levels of resources and associated skills available to undertake the required integration and customization activities?
- Are you clear on how you intend to manage these digital signatures, and for how long?

If you can provide suitable answers, you should be able to expect a vendor to provide you with realistic cost estimates.

IN THIS CHAPTER

- Seeing what has been signed
- Ensuring that archived documents remain valid
- Dealing with threats
- Understanding the legal implications
- Bringing customers along for the journey

Chapter 5
You've Signed, Now What?

Getting your organization up to speed with digital signatures is quite an accomplishment. But the journey is far from over. Your customers need to embrace the technology and understand how to use it. You need to ensure that what gets signed digitally stays valid as long as it needs to. You must understand the threats that could stand in the way of success, and deal with them effectively. And you need a solid understanding of the legal ramifications of digital signatures.

That's where this chapter is headed. It outlines the ways you can check on the signature status of a document, how you can make those signatures stay valid for the long term, and how you can keep unsavory characters from derailing your initiative. This chapter also explores the legal frontier upon which digital signatures have embarked, and ponders how consumers will embrace the technology as it unfolds.

Seeing What's Been Signed

REMEMBER

PDFs represent the one category of digitally signed artifacts you really need to know how to read. The PAdES standard specifies what a digitally signed document should look like, so they have a consistent look and feel.

Let's say you open the document in Adobe Reader. There are several key things you can't miss that indicate the document has been signed. See Figure 5-1, where they're circled. This is your first glance to see if everything checks out (or doesn't).

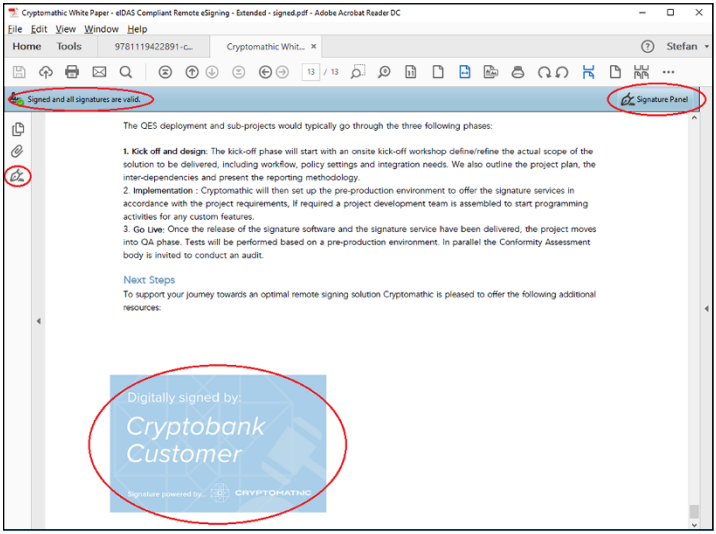

FIGURE 5-1: A digitally signed PDF following PAdES standards. This example includes an optional proprietary signature stamp.

To dig deeper, open the Signature panel, click the options icon, and then select Show Signature Properties. You'll get the option to view the certificate chain by clicking Show Signer's Certificate.

Once you've clicked that button and gotten to the next dialog box, click the Trust tab. This shows the full details of what the certificate was intended for, and if it passes the verification. The verification process needs no further information — you can do this offline.

Another clever bit of mathematics checks every necessary part of the chain, from the document text, through to its hash, its signed hash, and the whole certificate chain right up to the root CA certificate. With regard to that certificate, ultimately you either trust it or you don't. Adobe Reader knows which root CAs belong to a standard trusted list. Click the Summary tab to see where the root of trust is established.

If you're fortunate, you'll see the approved EU trust mark (the little blue padlock icon), as shown in Figure 5-2. That's reserved for Qualified Trust Service Providers and indicates that the signature complies with the eIDAS regulation for Qualified Electronic Signatures.

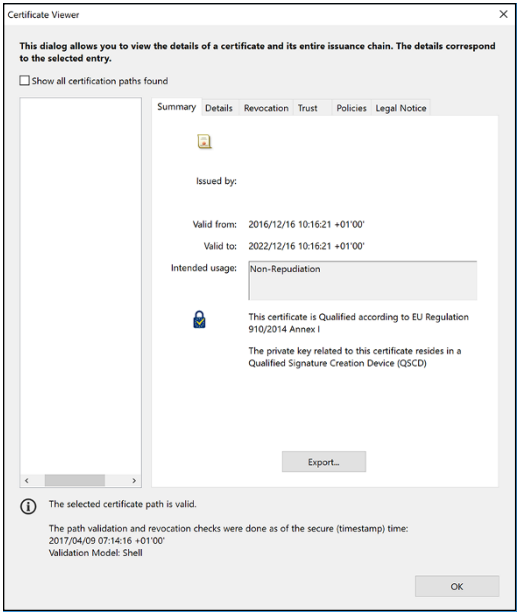

FIGURE 5-2: The "Summary" tab of a certificate in Adobe Reader. This one shows it conforms to QES for the eIDAS regulation.

Archiving for the Long Term

REMEMBER

You can store a PDF document for a very long time, which means there's a need for tools that will ensure electronically signed documents will remain valid for long periods. What if the signing key/certificate has been revoked? What if the issuing CA doesn't

even exist anymore? If you have an important document, you need assurance that the signature will remain valid.

There are several standards in place that attempt to solve that problem. They define how to archive PDFs under the PAdES standard.

PAdES Baseline Profile

The following relevant profiles are defined in the technical specifications:

- **B-Level:** This is a profile for short-term electronic signatures. It must include an electronic signature and the signing certificate.
- **T-Level:** This profile is like B-Level, but it adds a timestamp, a time-mark proving that the signature existed at a certain date and time.
- **LT-Level:** This one is like T-Level, but adds VRI (verification-related information) data to the DSS (document security store). In short, this profile enables a document signature to be validated even after a long period of time, even when the signing environment (such as the signing CA) is no longer available. The LT level is recommended for Advanced Electronic Signatures, but you'll need to check national laws on a case-by-case basis.
- **LTA-Level:** This builds upon the LT-Level, adding to the DSS a document timestamp and VRI data for the TSA (timestamping authority). An LTA form may help to validate the signature in spite of just about any event that may limit its validity. This is the recommended profile for Qualified Electronic Signatures.

Long-Term Archival with Timestamps (LTA)

The LTA level addresses digitally signed PDF documents that are stored for long periods, and it's very similar to a former profile named LTV (long-term validation). With the LTA level, timestamp tokens are incorporated into the PAdES signature that will allow for the long-term integrity and availability of the signed document.

TECHNICAL STUFF

To conform the LTA level, you have to meet not only its specific requirements, but also those of the B, L, and LT levels. Signatures that conform to the LTA level must have at least one document timestamp applied to their profile. Before the document-timestamp attribute is generated and incorporated into the signature profile, all validation material required for signature verification must be included. This material includes all certificates and OCSP or CRL status information pertaining to those certificates. This information is required to validate:

- The signing certificate
- Any attribute certificate used in the signature
- Any timestamp token's signing certificate that is already included in the signature

Using the PAdES Baseline LTA standard ensures the validity and integrity of signed PDF documents that might need to be accessed far in the future.

Here's another challenge for long-term preservation: What if signature algorithms that everyone trusts now lose their luster and are in the future considered weak? A signature kept in archive for an extended period of time could in principle be compromised. For example, a future exploited weakness — due to keys no longer being sufficiently large to resist new attacks on RSA signatures — may allow the document to be substituted without invalidating the signature.

TIP

To accommodate this concern, it's common to employ a notary to re-sign archived documents at intervals. The new signature will always be made using signature algorithms that are considered strong at the time, and because it cryptographically binds the archived document to the new signature, the signatures can be refreshed in this way.

This brings up the function of a validator or notary service, which receives a signed document and outputs a sealed validation report. The core functionality includes extracting the PAdES signature from a PDF document to perform the following operations:

- Check the document's integrity.
- Verify the signature value.

- Check the Online Certificate Status Protocol (OCSP).
- Check whether this signing certificate was issued from a trusted CSP issuing qualified electronic signatures such as an EU Trusted root.
- Validate the timestamp (where applicable).
- Display the name of certificate holder and certificate policy (Qualified, not Qualified, and so on).


REMEMBER

Even if you have no current plans to institute a digital signature system within your business, you should still be aware of techniques for managing such documents. You're very likely to receive them in the future.

Dealing with Threats

This subject is, of course, critical to deployment success, but what follows is just a basic overview, highlighting only the most important aspects.


REMEMBER

Security engineers talk in terms of *threat models* when analyzing a system for weaknesses. It's an impressive term that really means, "What's the worst that can happen, and how would it happen?"

A threat model isolates parts of a system looking for the key resources (sometimes called *honey pots*) that an attacker would want to access. Note the plural, "honey pots," because there may be more than one!


REMEMBER

The next term you'll hear from security engineers is the *attack surface*. That's the interface that is presented to an attacker before anything happens.

The relatively good news here is that for remote signing services, the threat model is very clear and well understood, and the attack surface is small. In fact, the entire back end of these systems will get certified, regulated, audited, and tested so much that no sane attacker would begin there. That's not to say that they are totally invulnerable, because smart attackers always focus on the weakest parts first.

So, the attack surface and main vulnerability are very clearly at the front end, which are the processes that the user interacts with directly on a phone, tablet, or desktop. The honey pot is to subvert the user's private key.

Hands off my private key!

Again, there's some good news. The threat model is not to steal the key. Sure, some bad guy could, but:

- It's virtually impossible to do that with the deployment of tamper resistant hardware (HSMs).
- And you don't need to, because the goal is to attack the *usage* of the key!

For remote digital signing, the keys are kept in hardware security modules (HSMs). This is hardware that is certified, regulated, audited, and tested to ensure that it will never let the keys be revealed to anyone or anything (except itself).

WARNING

But don't forget Security is A PAIN! The A in PAIN means "Authentication," and this is the hard one. This is the one that gets attacked first every time. If you can somehow fool the system and control authentication, you've won.

REMEMBER

The best systems, which are those certified to Qualified status, will raise the bar even further. Here's how:

- Not only will the HSM protect the keys, but it will protect the code that uses the keys. An attacker won't have a chance of subverting the code that uses the keys. It's called the signature activation module (SAM); it's a game-changer (but it's not cheap).
- The best systems also deploy certified authentication hardware at the signatory end. You may have seen those small hardware *tokens* before, such as the one shown in Figure 5-3.

FIGURE 5-3: Example of an authentication token.

These tokens don't protect the keys but they protect the uniqueness of each signing session. They generate a random number that is only known to the back end, which is the SAM code that runs on the HSM, securing the entire end-to-end session.

REMEMBER

So, when it comes to protecting the channel, you'll have an end-to-end encrypted, authenticated, even fully integrity-checked channel, secured at both ends by hardware that's fully tested and certified to the highest standards available. It's safe to say there are very few other commercial systems offering a more secure experience, while making it available to such a wide customer base.

The human factor

One thing remains, as it always does: the human factor. What this technology does is push the boundary of vulnerability out as far as it can go, to the human-computer interface.

TOKENS, BUT NOT SMART CARDS?!

You may be thinking, "If zero footprint is the be-all and end-all, and smartcards don't work in practice, why swap one piece of hardware for another?"

The reason is simple. The system offers much easier maintenance and key management. If a user's smartcard gets lost and a new one must be provisioned, that means generating new keys on the card, certifying those keys, and revoking the old ones. What's more, any interaction with the key management system needs to be audited and carefully managed.

If an authentication token (such as the one in Figure 5-3) gets lost, a new one is provided and the old one revoked, but there's no need to generate and certify new keys. In other words, because of the indirection from signing to authentication, this task is much easier.

And, don't forget! Your organization may already be using authentication tokens for securing access to online accounts.

The human factors look like this:

- **Remote signature service:** 100 percent controlled by "trusted" administrators according to best-practice principles of general high-level security administration. That means:
  - *Separation of duties:* There are clearly defined roles with functions that usually don't overlap.
  - *Dual control:* It takes at least two admins working together to perform any change of state to the system.
  - Strong two-factor authentication: Both a token and a password.
- **The trust service provider:** This is the certification authority. The trust is in the process by which the digital signature system gets certified. This is fully specified within eIDAS and can be independently audited.
- **The auditors:** You can assume they are trusted!
- **The user:** The user gets protected from many of the usual threats common to apps and applications, such as generic viruses, keyloggers, and trojans. Such mindless attacks

should gain no useful information from a digital signing transaction that a user rightfully intends to carry out. The best systems guard against replay attacks, for example. The two nastiest threats of all still have some power over the user, though. These are:

- Direct social engineering
- "Man-in-the-browser" attacks

Incidentally, you may have read reports about digital certificates being "stolen," as if they were a static resource. It's very misleading to talk about them that way, and doesn't help when trying to understand what happened and how it should be prevented. The attack on a certificate authority (or, for that matter, *any* organization providing a security service) is an attack on the process rather than acquisition of a static resource. The difference is not at all subtle. When a process is attacked, that always involves humans, while digital theft can be automated.

Direct social engineering

REMEMBER

You've no doubt become familiar with the technique of phishing and its even nastier cousin, spear-phishing. You may well have experienced it directly. A Qualified Digital Signature system will guard against these general attacks, because the random number-generating tokens ensure each session is unique, which means an attacker can't gain enough control.

WARNING

This pushes the attack boundary one step further out: the direct social engineering attack. This can take the form of, for example, a direct telephone call to the person in the middle of a signing transaction. The caller gains the confidence of the signatory in some devious way, perhaps pretending to be from the service provider, claiming to be testing the system. The caller takes the poor victim through a real but fraudulent transaction, all the while assuring that it's only a test.

TIP

How can you guard against this? If at all possible, train your customers, empowering them to always be in control of the session and be ready to quit at any point or to ask questions at any point. They need to know not to listen to anyone who tells them to go off the map. Design your UI so your customer has no reason to feel hurried, and remind the customer not to take phone calls during the session.

Man-in-the-browser attack

Unlike the secure code execution taking place in the certified hardware of the HSM, no one can truly trust any computer process anywhere anymore. It's just too easy to subvert. The National Security Agency has stockpiles of exploits it could unleash whenever it felt justified in doing so, and those exploits leak! Take ransomware, for example. It has come to be a pretty well-understood topic.

In the context of remote digital signatures, this problem can be characterized as the man-in-the-browser. That refers to a process on your device that has control over what happens in the browser.

The defense? It's what cryptographer Bruce Schneier calls "defense-in-depth," a layered approach of independent stumbling blocks for any attacker. Perhaps the most significant of these is multi-channel dependency. If you make it such that the number of independent things an attacker must subvert to win is two or more, this makes the job much more than twice as hard.

REMEMBER

The WYSIWYS concept developed by Cryptomathic does exactly that. It ensures that in order to complete the full signing transaction, multiple-independent channels must work together.

Legal Matters: Liability and Non-Repudiation

There's plenty of legal discussion in this book, but it's primarily from the regulator's point of view. What about the practical implications? What happens when there is a dispute?

REMEMBER

So far, very few cases involving digital signatures have gone all the way to a judgment, and only one recently. That was Case No. 16-22134-D-7, of the United States Bankruptcy Court in the Eastern District of California.

The synopsis in this case is that the law explicitly mandated the use of a traditional "wet" signature for case-supporting documentation in a bankruptcy case. The issue was not really a problem in the signing system. The issue was the use of the system

itself, given that California state law has an explicit exemption in certain cases.

This case points to the fragmentary nature of U.S. law. It's a situation that eIDAS would override by providing a much clearer framework. If the system had been Qualified and a similar case tried in the EU, there could be no reason to question the validity of the digital signature. Do you see why Qualified status is so useful now?

Here's the other issue. Even when the transaction is admissible, what if the client claims he or she never was involved in the transaction? This is the thorny issue of non-repudiation.

Non-repudiation in digital signature operations is like the phenomenon of phantom withdrawals of money from ATMs. The difference is that the hoops that must be jumped through to initiate a signing operation can be made much higher than presenting an EMV chip card and a PIN.

The X509 standard for digital certificates includes a "flag" (a bit of information) that indicates if the certificate can be used in a way such that its use cannot be repudiated. Experts have differing opinions as to whether this flag could ever have any meaning. That said, there has never been a more appropriate time to claim that it can have some meaning in a legal context. The technology has caught up with the intention.

Nevertheless, controversy remains. There are several reasons, not the least of which is that it has not been tested in law yet.

When using e-signatures, you can argue that they create a higher probative value for a signed document or transaction when using the eIDAS standard for a Qualified Electronic Signature (as well as the Swiss ZertES standard). That, in turn, provides strong non-repudiation.

REMEMBER

Why? Because eIDAS sets out the requirements for the systems and procedures that trust service providers must put in place in order to provide Qualified Electronic Signatures, including an audit trail. Under eIDAS, the proof for non-repudiation doesn't rely wholly on mathematics and cryptography — those technical aspects combine with the systems and procedures to create strong non-repudiation.

So, can non-repudiation be achieved? The answer is a solid "yes" when it concerns transactions in the EU or Switzerland, because QES has the same legal effect as a handwritten signature. There will always be arguments about how a system or process can be subverted or repudiated. But with QES, the liability is shifted to the user if he or she wishes to challenge the authenticity of an e-signature on a document or transaction. You can accept a Qualified signature in the EU or Switzerland with a high level of confidence that it cannot be successfully repudiated without substantial evidence, just as in the paper world.

WARNING

The United States, on the other hand, has no such regulation. That means there is no legally backed non-repudiation, which leads to high levels of uncertainty when signing digitally.

Getting Consumers to Buy In

So, it's a matter of technology adoption, isn't it? All consumers love technology, and can't wait to use it, right? Not necessarily.

In the UK it has been just ten years since the first contactless payment card transaction, and in recent years this technology has enjoyed explosive growth. There have been increases in the numbers of cards and contactless terminals, as well as the payment limit (now £30). There were reports throughout 2016 about the growth in mobile payment in the U.S., UK, and Europe.

Early in 2017, a UK report suggested many consumers have failed to take up Apple Pay, which launched in 2015, or Android Pay, introduced in 2016, while contactless payments more than tripled to more than £25 billion. With regard to mobile devices, it seems like a lot of users are hesitant to register for something new and create more dependencies on a device they love to exchange and upgrade frequently — why do so when a contactless card is just as convenient? And then there's the natural inclination of laziness. Life is full of priorities higher than signing up for payment through a mobile device, especially when there's an alternative that is convenient and hassle-free.

REMEMBER

Could digital signatures experience the same kind of hesitancy that has afflicted mobile payments? It's unlikely. Mobile payments don't offer much more than the use of contactless cards, but digital signatures, on the other hand, have something important to

offer that other mechanisms don't — a greater level of confidence and trust, and a substantial saving of time.

That doesn't mean digital signature technology will have a rate of take-up comparable to contactless cards. Digital signature technology is more subtle, but certainly reassuring if correctly deployed by organizations.

In recent years, many parts of daily life have been influenced by public and private sectors driving their services online or paperless. Credit card and utility bills, insurance policies and documentation, TV licenses, share trading contracts, user manuals for consumer products — all have gone online, whether users have wanted them to or not (sometimes users are penalized if they hold out).

The result of this push is that consumers have numerous logon identities for websites and portals. Overwhelmed users must keep up to date with difficult-to-remember passwords that have their minimum length requirements, the need for special characters, and seemingly frequent demands to be changed. It can be a real annoyance. Could digital signatures add to that noise?

REMEMBER

They don't have to. If your organization uses digital signature technology carefully in conjunction with your business applications, giving plenty of consideration to the overall user experience, these consumer or business users could become your brand advocates. If you achieve this and meet your overall business objectives — improved service levels, business agility, reduced operating costs, and so on — then embracing this technology has to be the right approach.

TIP

As an organization, must you digitalize? The answer is "yes," and depending on what industry or market sectors you're in, your competitors might make that decision for you. If your usual stance is to be a "technology follower," in this case you may want to consider becoming a "relatively early" adopter to gain advantage.

REMEMBER

You've probably come across this point several times, but it bears repeating one more time. The usage and implementation of digital signatures won't be successful solely because of technology. What matters most is how this technology works in partnership, or rather seamlessly in harmony, to support your organization's digital services. That's what's crucial to real-world success.

IN THIS CHAPTER

- Engaging expertise and original thinking
- Offering new and innovative approaches, features, and flexibility
- Demonstrating experience and dependability
- Breaking free of constraints

Chapter 6
Ten Ways Cryptomathic Can Help You

Chapters 1 through 5 assert that "digital signatures are essentially about *trust*." And they demonstrate why it isn't practical for an organization to own all the technology elements of its digital services.

With that in mind, what will enlightened organizations be seeking from their technical partners when providing digital signature services and technology? The answer is *confidence* that the partner will be able to assist in removing complexity and ensuring that initiatives can meet expectations. This chapter shares competencies and characteristics that Cryptomathic can demonstrate to deliver that C.O.N.F.I.D.E.N.C.E.

C for Cryptographic Expertise

With more than 30 years of technical and commercial success, Cryptomathic puts forth a solid claim to being experienced professionals in applying cryptography to business, whatever the delivery channels. Members of the cryptography team have invented and contributed to next-generation cryptographic solutions and algorithms, including the Advanced Encryption Standard (AES) endorsed by the National Institute of Standards and

Technology, and Elliptic Curve Cryptography (ECC). In addition, they have participated in research centered on electronic payment schemes, new hash algorithms, and more.

O for Original Thinking

Cryptomathic considers itself to be an original thinker in the application of cryptography to business. One example is the company's patented "What You See Is What You Sign (WYSIWYS) technology.

Another example is the provision of off-the-shelf solutions. The company's Crypto Service Gateway (CSG) can function as a cryptographic control center, acting as an HSM service and crypto policy management interface delivering and managing crypto for any application in your business.

N for New Approaches

Cryptomathic experts are always seeking to apply new approaches and techniques to the use and management of cryptography, incorporating the results into existing and new products alike. CSG, for example, was groundbreaking when it was first introduced almost a decade ago.

F for Features and Flexibility

Cryptomathic works in long-term partnerships with customers. The company recognized several years ago that there would be substantial and accelerating growth in the use of cryptography and encryption by businesses in applications and services. It was and remains evident that traditional methods of deploying cryptographic capabilities into business systems on a per-application basis would be costly, complex, increasingly cumbersome, and inconsistent in implementation.

Throughout Cryptomathic's products, you'll see features that enable proactive, flexible, and rapid management of cryptography within business applications. Products such as Signer, CSG, and CKMS (the key management system) all epitomize this philosophy.

I for Innovative Solutions

Cryptomathic is one of the best-kept secrets in IT security. The company provides innovative solutions, many of which are powering parts of the digital and Internet infrastructure of customers globally.

Cryptomathic Signer was the first centralized digital signature solution deployed on a national scale, many years before "cloud" became the norm. The company has several patents in this field, including WYSIWYS technology. The technological advancements in the digital signature space was the reason the World Economic Forum named Cryptomathic one of the 40 most innovative companies in the world.

D for Dependability

Cryptomathic was founded in 1986 and was one of the first companies in the world to commercialize cryptographic algorithms. The company has grown and evolved extensively through the years to remain at the forefront of security technology. It's all about preempting new requirements brought about by emerging technologies as well as changes in the risk profiles of technologies used in cryptographic algorithms or regulatory decisions (think Moore's Law). Cryptomathic recognizes that clients purchase products and services expecting to ease the management burdens that go along with increasing the use of cryptography in their businesses.

E for Experience

The Cryptomathic team is populated by experienced subject matter experts in the application of cryptography. It's a well-established global provider of secure server solutions to businesses and organizations across a wide range of industry sectors, including banking, government, technology manufacturing, cloud, and mobile.

Cryptomathic's pedigree, and that of its customers, is such that compliance with both existing and emerging technical standards and security best practices are topics treated seriously throughout the product ranges. Customers are able to achieve compliance to applicable standards more readily than might otherwise be the case.

N for Not Constrained

Cryptomathic is proud of its heritage, strong technical expertise, and unique market knowledge. It is a well-established and independent supplier of secure server solutions, and it isn't bounded by the constraints that certain hardware or computer operating systems can impose. This independence allows Cryptomathic to develop and evolve its products and tailor bespoke solutions to meet the exact requirements of customers.

C for Commercially Perceptive

As a specialist supplier in a growing and fast-moving marketplace, Cryptomathic has to be commercially perceptive and aware of the needs of customers and markets. Early business users of cryptography were banks and government, but now cryptography is regarded by many as cool and essential. The company's customers now come from an ever-widening range of industry sectors.

With this widening reach, together with recent moves to operating in the cloud, licensing models for software solutions have had to evolve. Cryptomathic's products and services cannot, by virtue of the facilities and functions they perform, be inexpensive. But Cryptomathic recognizes the importance of providing value to customers and is willing to discuss a number of commercial options to suit client needs. Those options can be linked to a number of business metrics.

E for Engineering Excellence

Cryptomathic has evolved extensively to remain at the forefront of providing security technology. A part of its DNA is a passion for affordable software engineering excellence. For more than 30 years, the company has been challenged many times by customers — perhaps in the use of new software techniques, meeting demanding and potentially groundbreaking transaction performance targets, and addressing security requirements. Many companies are long-time customers, which demonstrates that those challenges have been and are still being met.

Enable business with digital signatures

Digital documents are increasingly commonplace in today's business world, and forward-thinking organizations are deploying digital signatures as a crucial part of their part of their strategy. Businesses are discovering a genuine market demand for digital signatures in support of organizational goals. This book is your guide to the new business environment. It outlines the benefits of embracing digital signature techniques and demystifies the relevant technologies.

Inside...

- Advance your organization's digital strategy
- Provide strong non-repudiation
- Offer "what you see is what you sign"
- Ensure enhanced security
- Provide user convenience and mobility

CRYPTOMATHIC

Chris Allen is a Senior Solutions Architect at Cryptomathic and has been heavily involved with the development of Hardware Security Modules. **Steve Marshall** has more than 15 years' experience in deployment, enhancement, and strategic management of cryptographic systems at a global bank and more recently as technical advisor at Cryptomathic.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

for dummies®
A Wiley Brand

ISBN: 978-1-119-42289-1
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.