How to close the gaps in cryptographic certificate management

A view on all aspects of cryptographic security

Abstract

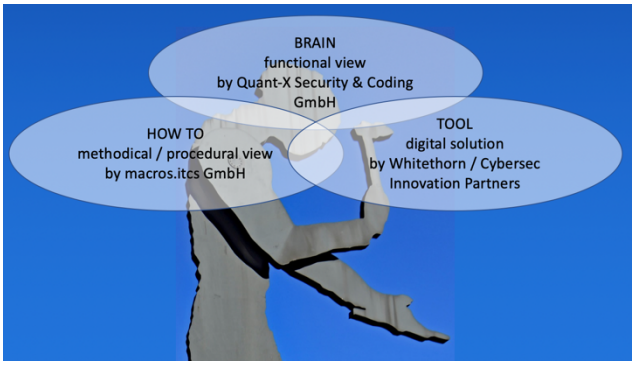
Cryptographic Certificates form the basis of all confidential content and authenticated communications in the landscape of dynamically initiated connections. Hardly any digital service works without them. Even for the delivery of public information we need cryptographic certificates to ensure that the content is not only original, but also sanctioned by the authors and publishers.

The internet is just one example of an infrastructure in which we rely on trust verified by cryptographic certificates, yet the best example of how publicity and CIA (confidentiality, integrity and availability) cannot be separated from each other anymore. On the other side we have private or state infrastructures which hold highly secret information for dedicated persons, groups or institutions.

Certificates define the ownership of a digital service as well as the scope of their validity. The certificate type for a digital service is chosen according to its intended trust reach. These two facts imply bidirectional impacts of certificates regarding security, in a positive and a potential negative sense.

A sensitive handling of certificates is not only based on technical, but also on human behavioural aspects. The resulting need for efficient and sensible cryptographic certificate management raises questions about digital solutions as well as procedural definitions tailored to the concerning infrastructures and the involved staff. Decisions concerning both aspects are based on sensible information security and risk management.

Quant-X Security & Coding is responsible for the functional view, the Macros Group covers the information security and risk management and procedural aspects based on 20 years project management experience in the financial sector and Whitethorn, from Cybersec Innovation Partners, comes with a digital solution for the challenges posed by the multidimensionality of certificate management in complex infrastructures.



History of Cryptographic Certificates

For thousands of years all cryptography was symmetric, meaning that the keys for encryption and decryption were identical. The secrecy of this communications relied on safely sharing the key with a communication partner, usually by meeting them in person or by setting up a system for knowing when to use which key for a secret communication.

The need for secure instant key exchanges came with the dawn of dynamic information systems in the late 1970s. Asymmetric cryptography provided the answer - cryptographic procedures like Diffie-Hellmann and RSA were born. These procedures are still being widely used, and successors like New Hope and NTRU are currently evaluated for standardization by the NIST. In asymmetric cryptography, we have two distinct keys, a public key for encryption and a private key for decryption of data.

Cryptographic Certificates define the ownership and the scope of a public key. They can be shared publicly, because they can only be used to create secret information, not reveal it. Furthermore, they can be used to verify a digital signature, therefore verifying an owner and the integrity of a received digital message.
There are two ways of verifying validity of a cryptographic certificate, centralized and decentralized. The centralized issuance and validation of certificates is realized by Certification Authorities, instances, which are themselves audited by dedicated organizations. Examples of decentralized validation are web of trust or Blockchain-based systems like CertCoin. In this paper we focus on centralized validation of certificates.

Evolution of Cryptographic Certificate Management

Since cryptographic certificates are used in digital infrastructures their application, as well as the management, has changed. Originally, each administrator of a digital system or service was responsible for its cryptographic aspects. Even in complex infrastructures, the certificate management is still often handled in an uncoordinated way. On the other hand, it is often a nuisance for IT-operational staff to be aware and keep a record of the state of the cryptographic certificates used in their systems.

Cyber Crime has found various ways to attack encrypted services, which has led to serious data breaches in the past few years. One of the greatest vulnerabilities in this regard are invalid and expired certificates. The costs coming with these data breaches created pressure in the economy to implement security mechanisms which prevent a system from communicating when the certificate is no longer considered valid.

The negligence of certificate management in combination with these security mechanisms produce business interruptions by failure of digital services, which come again with potentially high costs. In certain cases, it can take weeks to renew a digital certificate after its expiration. Besides that, the reputation of a company might suffer seriously from such incidents.

A sensible and efficient certificate management is the solution for breaking the cycle of unnecessary costs and security issues around the necessary usage of cryptographic certificates.

Risks

Weak cryptographic certificate management comes with many risks, beginning with key generation in an internal public key infrastructure and ending with the revocation of trust of an official Certification Authority (CA).

The latter can happen instantly and result in an avalanche of revoked certificates issued by the CA. The revocation of trust of the DigiNotar certificates was the proof that this kind of scenario can become a real threat to global businesses.

Examples of further risks are;

- weak algorithms in certificates
- invalid or insecure key generation
- insecure distribution of private keys
- unauthorized access to private keys
- no responsible staff
- unavailability of responsible staff
- choice of wrong certificate type for system or application
- unrevoked certificates of inactive systems
- unavailable revocation lists

Another hardly considered risk is posed by the fact that some companies, namely in the financial sector, implement SSL-scanning for detection of malicious content. This can only be implemented as an unauthorized or authorized “man in the middle” attack, a mechanism which is intended to be impossible in profoundly secure cryptography.

With TLS 1.3, all algorithms which enable unauthorized “man in the middle” attacks were eliminated. The circumstance that many companies still insist on the usage of TLS 1.2 implies that SSL-breaking is still realized in an insecure manner. We recommend looking at those mechanisms as well.

A View on Certificate Management in Enterprises

Certificate Management from a Certification Authority point of view is considered in the Certification Practice Statement (CPS). The CPS is the document from the CA, which describes their practice for issuing and managing public key certificates. Questions with regards to embedding certificate handling in an enterprise are not covered by those documents.

A huge IT-provider for example has to manage certificate orders for various customers from different Certification Authorities. Some enterprises issue their own certificates for internal systems and applications, with or without root-signing, while they use certificates from official Certification Authorities for public applications. Delegated sub CAs might be present as well. To get an idea there might be hundreds of thousands internal and public certificates of various types handled by more or less technically adept staff working in different departments and companies.

From an enterprise point of view it makes sense to link the legitimate type of a certificate for a system or an application to an IT service. Directives about where and how to order the right certificate, report irregularities such as the suspicion of a compromised private key, etc. have to be tailored to the needs and infrastructure of an enterprise. Last, but not least, those directives have to be communicated to every responsible person in a binding way.

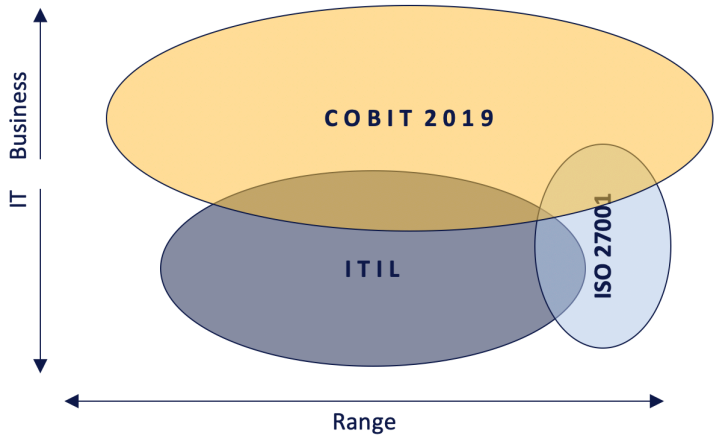
Best algorithms and techniques can only be as safe as the processes and environments in which they are embedded. Therefore, it is necessary to build organizational and functional structures that ensure secure and predictable handling of cryptographic environments. This includes views on information security management as well as views on information risk management. Each view defines requirements as well as to contain objectives and controls.

To create holistic approaches, there are several international frameworks that support creating and implementing such management systems. Macros.itcs prefers a combination of the frameworks:

COBIT 2019 provides a holistic, dynamic and tailored governance system for information technology. It includes control objectives for managing security and risks on a business level.

ISO 27001 focuses on information security. It complements COBIT and provides guidance on a more detailed level.

ITIL delivers a broader view on IT services over their life cycles.



In addition to mentioned security views, there are economic opportunities by aligning structures and processes to such frameworks. Especially COBIT is designed to ensure benefits delivery and resource optimization.

Efficient Digital Certificate Solution

Cybersec Innovation Partners (CIP) are a team of recognised cyber and security leaders led by industry specialists. CIP include among their number Don Randall, former Head of Security at the Bank of England, Andy Watkin-Child, a former member of Santander's Global Risk Leadership team and Paul Foster, former Global Head of Cyber security at HSBC.

PKI/Certificate management is totally dependent upon the certificate management's full visibility which, until now has simply not been possible. Fractional visibility provides only fractional management which is why so many companies, including Tier 1 Banks and Technology giants like Microsoft, Google, Adobe, Citrix and many others have certificate issues resulting in service outages, vulnerabilities and breaches through compromised certificates that are not identified.

Whitethorn® provides full PKI visibility and is the only digital certificate and key platform that provides full discovery, management and automation of all SSL/TLS/PGP and SSH certificates and keys. Whitethorn® provides comprehensive certificate lifecycle management, including origin, cipher strength, access, device and software identification. Whitethorn® is the most comprehensive cryptographic management solution with automation technology. Its next gen capability is unrivalled providing full visibility and management of what was previously considered impossible.

Whitethorn® goes beyond the capability of any digital certificate detection and management product on the market today. It reduces the attack surface across your entire enterprise, saving your company £millions in costly service outages, data loss and securing your infrastructure, vastly reducing your risk.

Conclusion

Cryptographic security in digital infrastructures of enterprises is usually covered by heterogeneous PKI landscapes. The variety of the types of certificates handled in those landscapes increase the complexity of an efficient and seamless certificate management. Responsible staff work in various departments of an enterprise, sometimes even in other companies.

Whitethorn® from Cybersec Innovation Partners includes features which address all mentioned challenges such as:

- APIs to CAs for automatic certificate renewal
- Certificate Discovery on an agent or agentless basis
- Central database and management GUI

For further information find the Whitethorn® brochure, datasheet and whitepaper at https://www.cybersecip.com/whitethorn.

Quant-X Security & Coding provides a technical and functional analysis of the digital infrastructure. Macros.itcs offers information security and risk management based on this analysis. Together we devise a company-tailored solution covered by the tool and defined responsibilities. This includes adjustments to processes and guidelines as well as the technical and procedural implementation of the tool.

With this approach we can provide a holistic solution for a PKI/Certificate management with maximum PKI visibility within minimal system load and to achieve the highest possible automation grade tailored to the needs of enterprises.

About the Authors

Xenia Bogomolec
Founder of X-Quant Security & Coding GmbH
https://quant-x-sec.com
xb@quant-x-sec.com

Günther Heiß
Managing Director and Owner of Macros.itcs GmbH
https://macros-itcs.de
guenther.heiss@macros.de

Andrew Jenkinson
Group Chief Executive Officer at CyberSec Innovation Partners
https://www.cybersecip.com/whitethorn
andrew.jenkinson@cybersecip.com