[T71]: Security of electronic passports and national ID cards

Home exam

Candidate number: 15363

December 13, 2022

Introduction

The need for authentic, secure and valid identity documentation is essential to everyone in almost every aspect of life (such as operating your bank account, travelling, applying for jobs etc...). But in the face of technologic advancements the security of these ID-forms are prone to be malevolently comprimised. You might already be thinking of types of ID document dissasters concerning the missuse of important ID types such as passports and ID cards where the potential damage could be dramatic and to some degree very expensive/almost immutable. However, there are mutiple rutines, methods and techniques to prevent threats, and secure the documents where as the use of cryptography, hashing, PKI and digital signatures are some of the few. This paper wil not cover every framework detail within the manifold of passport and ID card security, but rather give

a solid understanding of the foundation to the matter. Lastly there will be discussions regarding strengths and weaknesses of existing structures and methods with suggestions of implementations to new or perhaps better suited ones.

Symmetric and asymmetric cryptography

In short cryptography is traditionally, a method for assuring confidentialty protection of messages/information in transit between two parties. If there exists a fraudulent third party the cryptographic techniques assures full secrecy of the information as long as the essential fingerprints(digital keys) are not astray. The encryption process is a concept where the secret message (plaintext) is encoded by using a so called key to prevent eavesdropping. Furthermore, there are two variations of encryption which is the title of this section, in fact symmetric and asymmetric encryption.

Symmetric cryptography is the simplest form of encryption where the same key is used for both encryption and decryption. The disadvantage is that both the sender and the recipient must share the same private key such that the secret information can be encrypted and decrypted. This makes the process prone to eavesdropping, since the actual key needs to be distributed and is the only key securing the encrypted session. With asymmetric encryption the issue is more or less solved, but with the expense of being a lot more difficult since it relies on the two communicating parties having full trust in assuring the secrecy of each others fingerprints. In simplified terms the algorithm is based of a so called key-pair where the sender and recipient generates a private-public key pair corresponding to each other. This way no theoretical third party can decrypt the given information as the recipient

being the only in possesion of the secret private key corresponding to the senders public key. Moreover, this public key cryptography can be showcased trough something called the RSA-algorithm which is quintessential in securing modern passports and ID cards.

Modern day passports and ID cards are what we call **eMRD/eMRTDs**(*electronic Machine Readable Documents/electronic Machine Readable Travel Documents*)[1] [1] which serves the purpose of authenticating who we are as an individual, through biometrics and other information elements identifying the holder and issuer of the ID document. The data stored on the chip of the eMRDs are strongly secured by cryptographic algorithms as mentioned, but there are certainly more intricacies to the matter. In the context of ePassports every issuing State has a minimum of two types of key pairs(A **Country Signing Certification Authority** (CSCA) key pair and **Document Signer Certificate** (DSC) key pair). When issuing an ePassport, the CSCA digitally signs the DS certificate throug a private key. Then the DS private key digitally signs the ePassport. This marks what is called the **Chain Of Trust**[2]. The inner workings of the chain of trust relies heavily on the security behind the root, CSCA, which is emphasized through how an eMRD is authenticated. When an eMRD is passively authenticated (through an electronic machine capable to read the information of the document) the chip of the document is scanned thorougly such that its possible to verify if the document is signed by an authentic DS corresponding to the correct issuing authority. While the DS certificate is being verified the machine also matches the DS to the corresponding CSCA. Since the CSCA signs the DS there is no way to either counterfeit or repudiate the DSC without also using a comprimised CSCA, since the CSCA is the

[1]Specification by ICAO Doc 9303 Part 1 - 12

root of all verification control. If by any means the CSCA is comprimised or tampered with, the consequences are catastrophical. This is due to the CSCA being the anchor in the chain of trust and a bilateral exchange object. That is also why the DS certificates are generated and used for periods of three months, as with the CSCA certificates between three to five years, in prevention of massive fall damage.

With the established overview of the chain of trust, it is reasonable to dig a little deeper into the sheer cryptographic techniques lying underneath the whole process. The RSA-algorithm is a founding part of most public key cryptography (asymmetric cryptograhpy) where the algorithm is based of a corresponding key pair between the sender and recipient. To demonstrate the usage of such an algorithm we divide the eMRD authentication into two phases. First is the enrolment phase which involves an application either live or digital, depending on policy by the issuer [2]. In this phase the applicant will get the information enrolled either through a so called biometric-booth or a website (again depending on which country the holder is from). From this action the holder will either recieve an entitlement, or not, based on the application. The application is signed by the DS. If the application is issued, there will automatically be generated a datapackage corresponding to the information elements of the application, where the data will be further processed using the RSA algorithm for the encryption part. This encrypted data will be stored in the RFID-chip (Radio frequency identification) on the eMRD together with the parts of a public key belonging to the DS. The RFID functions as tracker and identifyer of information tags stored on the chip of an eMRD.

[2]Live enrollment is for instance mandatory by law in Norway and Sweden

During the authentication phase, the eMRD is scanned with the public key being validated through a link comparison with the DSC‘s private key, certificate and the CSCA‘s public key. The DS certificate is issued by the Country signinig certificate authority. If by any means an eMRD contains more than one DSC these can be compared against their private keys and the CSCAs public key such that the possibilty of a forged DSC is next to impossible. For further mention this process is embedded under the **RSA-OAEP** (RSA-Optimal asymmetric encyption padding) scheme which in short is an encryption scheme using a form of Feistel network combined with the principle of the Diffie-Hellman key exchange method to prevent chipertext attacks and to build an all-or-nothing transform. Chipertext attacks are difficult to carry out, but with some insider threaths/knowledge and the known origin of the chipertext the attacker could potentially harm the certificate infrastructure (CSCA, DSC). To make the RSA-OAEP optimal it is recommended to implement the SHA-3 or SHA-5 (SHA: Secure hash algorithm) to the hash functions used in the scheme, where as SHA-1 is considered insecure due to being prone to collision-attack against well-funded opponents[3].

Lastly in this section it is worth mentioning the prospect of active authentication. Active authentication in the context of eMRDs is revolved around cloning detection and prevention, detecting whether or not the RFID-chip has been copied. It is important to realize that the passive authentication process only validates the information read from the chip is signed by the issuing governement. Albeit this secures the authenticity and integrity of the information within the chip, it does not prove if the information was read from a legitimate eMRD or not. With active authentication the process invokes a challenge on the eMRD which the holder has to sign with a

given private key stored in the chip (a password for example). The public key corresponding to this private key can then be used to verify the authenticity of the signature. This public key is part of the chip data signed by the issuing country.[4] With that said, it is reasonable to understand that this prospect of active authentication can be transformed into a valuable three-factor authentication method. Consider the following proposition where, the authentication process contains: Something you are (biometric data), something you have (passport, ID card, other security tokens) and something you know (password or PIN). By applying a private password or PIN to the already established authentication process, it can evolve the ressilience against forgery or cloning by signing the data package within the RFID with a personal private key corresponding to the holder by increasing the factors of authentication to three.[3]

PKI and key managment

With over 100 State and non-state entities issuing ePassports, and several countries issuing other forms of eMRDs, the necessity for secure cryptographic algorithms, policies and management is unquestionable. How to structure and behave in such a manner, comes through something called PKI (Public Key Infrastructure), which as the name reveals is an infrastructure or ecosystem based on policies, procedures and distributions founding a basis for how all information security structures should work. In the essence of eMRDs there has already been mentioned some levels of PKI, regarding the CSCA and the DSC. The CSCA is a certificate authority

[3]The ICAO application within the RFID-chip of ePassports, relies on verifying the presence of active authentication as well as if it is in use. Likewise does it also verify the functionality of the active authentication process. Usually a more precise term for such an application is chip authentication.

which in the PKI hierarchy is a root entity issuing digital certificates. Such an entity allows other relying parties to rely upon other signatures made about the private key corresponding to the certified public key. Coupled with a certification authority the structure also needs a registarion authority (RA), whom handles the request and authentication of entities requesting digital certificates. If a certificate issued by the CA is either suspended, declined or rejected the RA will revoke this certificate and order it in a **CRL** (Certificate revocation list) such that it is clear which certificate is to be trusted and which is not.

Taking a closer look at the design of a general PKI ecosystem it might look as follows[5]

- A certificate authority (CA) (Storing, issuing and signing digital certificates).
- A registration authority (RA) (Registering and identifying entities requesting a digital certificate and handling the CRL)
- A central directory (highly secured location where keys are stored, logged and traced)
- A certificate management system (System of managing access to stored certificates or certificates to be issued).
- A certificate policy. (Standarizing the PKI‘s requirements for issued certificates combined with assuring the trustworthiness of the PKI).

Among these design levels there are parts which are indesputably integral to the infrastructure (such as the CA and the RA). But even though a term like “central directory” sounds insignificantly less valuable than a certification

authority, there would undoubtly be a collapse in the confidentiallity and integrity protection of every certificate issued by this authority if there were to be no system of controlling and storing the essential fingerprints (digital keys corresponding to each certificate and digital signature in this matter). One way of governing such a layer is through a **HSM** (Hardware security module) which as a physical computing device manage and safeguard all digital keys stored from both the CA and the RA. Additionally the HSM offers fundamental features such as full audit logs and log traces, and secure key backup, which means every change made to the keys stored or managed by the HSM are carefully traced. If perchance there are issues regarding the keys, the HSM will safely generate backups to compensate for holes in the structure. So on a general note the HSM is pretty useful, but how essential is it in the context of eMRDs?

With the established understanding of how the information in an eMRD is translated when going through the authentication phase there are certainly many factors which in theory could go wrong. The worrying issues around data protection regarding the digital signatures, biometric data and digital certificates are mainly headlined even though a CSCA and DSC offers sufficient protection and authenticity. It is at this point countries around the world implement HSMs to further structure, control, manage and operate their PKI enviroments within the network of eMRDs. With true hardware security modules the issuing countries have full maintnance of the integrity of the keys through key management. This sort of key managment creates and stores keys for exclusive use within the confines of the hardware security module to prevent possible compromise.[6] To further prevent from insider threats the operation of HSM provides multi-factor authentication or multi-people authentication which is a necessisty

rewieng the intricacy of having multiple insider threats in the authentication process. By emphasizing the area of application of HSM techonology in the eMRD infrastructure it is valuable to discuss the properties of authenticity regarding self-signed certificates. When authenticating an ID document, the adequate asymmetric cryptography can be used in software without the need for HSM(since the key purpose of a HSM is to store and protect keys). For instance does every inspection system have the sufficient cryptographic processing capabilites to validate and authenticate the chip. However, while this may apply to the DS due to being signed by the CSCA, there emerges a conflict with the CSCA certificates since they are self-signed. By being self-signed the implication of not being certified by a higher-authority arises. How can one then fully reassure themselves that the CSCA is authentic? Well for one obvious fact the aspect of full audit logs and log tracing is a must since audit logs snapshots a given state of the CA, hence searching for irregularities in the CA(i.e. change in digital signature or tampered information). But there is also an indispensible value to keep the confidentiality, integrity and authenticity protection intact when either storing or exporting the certificates through the national PKD(Public Key Directory) and the inspection server, combined with transmission between other entities/countries and dissemination to the respecting inspection stations. Why? Well the argument is simple seeing that the authenticity, confidentialty and integrity of the CA must be absolute in every action it is being either checked or verified against. A way to meet this demand, is by using a SSL(Secure sockets layer) or more precicely a TLS(Transport layer secuirty) channel with both client and server authentication. Although this is not explicity imposed by any authority there is no reason to doubt the daily application of it and through a HSM this is fully functional. For

instance does the HSM have additional purposes such as *secure storage of CSCA certificates in the national PKD and inspection systems (HSM-stored)* and *storage of TLS server private keys in national PKD and inspection systems*[6], which implies that the authenticity of the certificates stored and transmitted via directories are fully secured due to no other uninvited entities having either acess or capability of tampering with the concering certificates.

By finishing off the section it is benefical to discuss a prospect of further improving the services in PKI. The utmost important question is then how we could at all times assure full trust in the root of our PKI (then reffering to our CA and RA) while yet maintaing effcient procedures and methods. Looking back on the last 15 years of PKI there has been immense shifts in the practice of layering integrity, authenticity and confidentialty through all levels of the infrastructure ecosystem. To somewhat reassure this requirement is through an audit. The audit is essentially an independant assesment controlling the quality of a system. However, there has been established regular audits reports regarding CAs to ensure that the CAs still meet the requirements needed to be fully trusted. If the audit is incomplete then the respective CAs know how to improve themselves, following the assesment/review criteria which could vary form backup-procedures, to adequate secuirty protocols (i.e. cryptographic protocols, HSM etc...) and secuirty policies. Although this seems organized and complementary there are certain issues to be considered such as how reliable and objective the reports are (taken to account who writes the reports), and whether or not the audit company is trustworthy since the CA is the companies client. One could consider hiring the same audit company not engaged by the CA, but seeing as though the company being hired by another independant

party may strongly decrease the level of favouritism in creating true reports. Further one could argue about increasing the number of audits to enhance the overview of the respective CAs functionality, but an audit only gives a portion of the CAs situation which is problematic giving there must be a full trust to the CA in realtime.

What then is there to iniate as a benefical factor strengthening the CA? For one fact, one could implement linked CAs. Linked CA means that the current CA private key is linked to earlier used CA-keys with a link-CA certificate. A link-certificate is formed by rekeying the current CA, to issue a new CA key also signed by an earlier CA key, such that if the question of authenticity arises the given country could verify the authenticity of the current CA key by verifying it against the link-CA, and ergo earlier CAs. This would additionally help the issuing countries detect if the CA is comprised such that no other entity could issue a certificate for themselves in the name of other countries or members. Building on the idea it might become evident that the method could result in a form of certificate transparency (CT) where the idea of logging new and older CA certificates in an append only list is highly substanstiable. An append only list is a form of computer storage where new data can be appended, but the existing is immutable. In this sense the issuing countries have a more structured and pinned overview of their publicly known certificates, while still ensuring that the log is honest.[4] Checking for honesty in the log is rather efficient since one could compare snapshots (the state of the log at a particular time) searching for inconsistencies, signalizing dishonesty.

[4] The log reffered to here is composed of a Merkel Tree/hash Tree,
which is an effecient and secure algorithm for verifying large datastructures.

Digital signatures and certificates

Having discussed cryptographic algorithms and their applications in eMRD secuirty through the CSCA and DSC, its only reasonable to further explore the topics of digital certificates and digital signatures. A digitial signature is a form of electronic "fingerprint" using mathematical techniques. In an encrypted message the digital signature marks the authenticity of the message such that the recpient is fully aware of its known sender, and also protects the integrity of the message seeing the information was not altered or tampered with during transit. Non-repudiation is a further aspect only mentioned, but not explicitly discussed which in the matter of digital signatures is very important. With non-repudiation an entity which has signed some information cannot deny to having signed it. In other words this does not give any fraudulent party the possibilty of faking a signature, even though they might have the access to the public key. Digital signatures use a standard and accepted format called PKI such that it follows strict legal regulations and provide high level assurance of the signer‘s identity. Usually the signatures are used to implement electronic signatures (eSignatures) which involves data getting consent or approval on electronic documents. In countries of the European Union electronic signatures have legal significance. Furthermore, are the digital signatures extremely important in the context of digital certificates since the signature corresponds to an entity(issuer) verifying the contents of the certficate. A digital certificate is as stated earlier an electronic documet used to prove the authenticity and ownership of a public key originating from issuer of the certificate.

In relevance to the eMRD the digital signature comes in handy when the

document is passively authenticated. Embedded in the chip, there exist a file or data package, namely the SOD (Document Security Object) which hashes all files stored on the chip (biometrics etc...), together with a digital signature of these hashes. The signature is as refrenced to the CSCA and DSC made by signing it indivdually with a private key corresponding to each other. In case a file on the chip (fingerprint, issuer, picture etc...) is changed this can be detected effectively since the digital signature changes due to the hash values changing. The reader authenticating the document also needs access to all public keys issued by the country corresponding to the documents private keys, such that it is possible to check if the digital signature is generated by the correct issuing country. However, seeing these procedures apply to ever, member of ICAOs PKD there is an obvious issue regarding non-participating countries. If an anomaly arises in the digital signature of a falsified passport belonging to a non-ICAO member, the inspectors may not detect the fraud due to the signature not being coorelatet to any keys stored in the PKD. One could consider applying active authentication in the previous scenario, by trying to link the holders private key to the public key correspondant to the digital signature and compare it to the actual public key in the PKD. Moreover, there are also rules stipulated by ICAO demanding a biometric authentication to initate a digital signature of audit logs, linking biometrics to the trusted staff members undertaking the enrolment of the eMRD belonging to the holder.[7] Which in a canny way could be linked to the signature on the eMRD chip, thus making it way more complex forging or tampering with a document.

With 193 membering countries of ICAO (as per June 2020) [8] there are certainly an abundance of digital certificates in circulation. To manage

and store these certificates safely, both ICAO and the indiviual members have something called a Master list. The Master list is essentialy a storage of CSCA certificates both self-signed and produced by the issuing country as well as every certificate the issuing country trusts.[8] In layman terms this mean that every membering country can bilaterly exchange CSCA certificates. When publishing the Master List other reciving countries obtain a set of CSCA certificates, in such a way that there is no need for bilateral exchange with each of the issuing authorities represented on that list. In further support of bilateral distribution there is an optional entity called the Master list signer that digitally signs a list of CSCA certificates (both domestic and foreign). The Master list also has the property of being able to distrubute link-CSCAs as well as CSCA self-signed root certificates which as discussed offers tremendous detection advatanges and relieveng countries of authentication conflicts at inspection routines. Though this certificate infrastructure seems secure, detective and effective there is one issue, which in the event of a fatal comprise could destroy the whole infrastructure of all eMRDs. The issue reffered to is the validity of public keys of the CSCA and DS. Validity of the CSCA public key is between 13 - 15 years which is fine since the private key needs to be re-keyed every 3-5 years and the CSCA is usually extremely well protected (although the validity should be shortened with a couple of years to fully avoid serious reprecussions). However, when turning to the DS it states that the validity of the private key is three months (good), before the need to re-key, and the validity of the public key is "approx." 10 years. Firstly the term approx is way to flexible meaning some countries actually extend this boundry even further(though not many). But the serious issue is that the ratio between re-keying and the public key validity is way to substancial. The DS is far from

as secured as the CSCA meaning that potential comprimise is way more likely. Assume the following, where an average amount of issued eMRDs per month is (between 50 000 to 100 000) a month per issuing country. In a years time the amount would raise to 600 000 and 1 200 000 and so on. If there is to happen a fatal compromised within the public key validity of the DS and the CSCA that would mean millions of eMRDs completely vaulnerable to serious damage and id-theft, without mentioning the colateral damage to all countries in bilateral exchanges with the exposed country/countries. Therefore as a conjecture or presumption, the reasonable validity of the DS public key should as long as the private keys validity, thus three months. According to ICAO the amount of eMRDs issued in the space of re-keying, only is about 100 000 - 150 000 documents per issuing country[9], which is only a small fraction compared to potential millions.

Conclusion

Seeing technology advance may scare many due to not having the same physical access and understanding of their ID documentation. But it must be clear that even though technology is advancing, the advancements are rather slow and time-dependant. Prior to around 2010 there were no methods for active authentication (chip authentication) to detect cloning of the RFID-chip which as it stands today is almost a mandatory excercise in every country issuing electronic ID documents. Proper machines for the reading the documents were in a primitve state (and not really implemented as a functional process) before the end of the decade thus implying it took almost ten years to fully issue a solution working on a day to day basis. Not only does that emphasize the time-consuming process of implementing

modern solutions to eMRD security, but also the contrary concering missuse and malevolent acts through the established security structures.

Through our current cryptographic algorithms (mainly RSA and elliptic curves) combined with the roles, policies, management, hardware and software designed by the public key infrastructure the protection of all valuable assets (electronic documents, certificates etc...) is highly impregnable. Though to be noted there are potential of improvement concering the process of authenticating the CSCA, seeing the self-signed conflict arise in many contexts. Where certificate transparency is a bold, but interesting train of thought in maintaining a realtime view of the certificate authorities. As well as maintaining an up to date view of all important certificates, there are just as much a priority to protect and maintain security of all issued documents by an issuing country. By adapting a validity period for all public and private keys signing issued documents the event of comprimise is largely reduced, but not fully extinct. This is where the issuing countries should implement a smaller ratio between the DS private key validity and public key validity since millions of eMRD‘s are issued in a 10 year period (considering on average a country issues between 100 000 and 150 000 eMRD‘s per three months). With that said and finishing off the paragraph it should on an international basis be achieved a three factor authentication process when inspecting an eMRD. By linking a personal password or PIN to the chip on the eMRD the process of either cloning, forging or decrypting the information stored on the chip becomes remarkably more tedious.

Bibliography

[1] International Civil Aviation Organization. *DOC 9303, Machine Readable Travel Documents.* Seventh Edition. International Civil Aviation Organization, 2015.

[2] Internation Civil Aviation Organization. *Cryptography 101, Basics of ePassport secuirty.* Internation Civil Aviation Organization. `https://www.icao.int/Security/FAL/PKD/BVRT/Pages/Basics.aspx` (accessed 5.10.2020).

[3] Wikipedia. *Optimal Encryption Padding.* Wikipedia `https://en.wikipedia.org/wikiOptimal_asymmetric_encryption_padding` (accessed 7.10.2020, last updated: 21 January 2020, at 12:19)

[4] READID. *Cloning detection for ePassports.* READID. `https://readid.com/blog/Cloning-detection-for-ePassports` (accessed 3.10.2020, published Feb 21, 2018, last updated: Updated 22 oct 2019 with status PACE).

[5] Wikipedia. *Public Key Infrastructure.* Wikipedia. `https://en.wikipedia.org/wiki/Public_key_infrastructure` (accessed 8.10.2020, last updated: 20 September 2020, at 18:22).

[6] SafeNet. *E-Passport: Deploying Hardware Security Modules to Ensure Data Authenticity and Integrity for Electronic Passport Projects.* SafeNet. `https://www.slideshare.net/SafeNet/epassport-deploying-hardware-security-modules-to-ensure-data-authenticity-and-integrity-for-electronic-passport-projects` (accessed 9.10.2020, Published: on Jun 10, 2011).

[7] International Civil Aviation Organization. *DOC 9303, Machine Readable Travel Documents, Part 9.* Seventh Edition. International Civil Aviation Organization. p.36, 2015.

[8] International Civil Aviation Organization. *Member States.* International Civil Aviation Organization.
https://www.icao.int/about-icao/pages/member-states.aspx
(accessed 21.10.2020)

[9] International Civil Aviation Organization. *Document Signer.* International Civil Aviation Organization.
https://www.icao.int/Security/FAL/PKD/BVRT/Pages/DS.aspx (accessed 21.10.2020)