

VOTING Stimmunterlagen Offline

Cryptography

Author	Abraxas Informatik AG
Classification	public
Version	1.1
Date	April, 5th 2023

Contents

1.	Introduction	3
2.	Key Exchange	4
2.1	Sender.....	4
2.2	Recipient.....	4
2.3	Signature Key Exchange.....	5
3.	Cryptographic Primitives	6
3.1	Key Material	7
4.	File Format	8
4.1	Conventions.....	8
4.2	ABNF specification	8
4.3	Example.....	9
5.	Encryption	9
5.1	Overview.....	9
5.2	Detail	10
6.	Decryption	11
6.1	Overview.....	11
6.2	Detail	11

1. Introduction

The VOTING Stimmunterlagen Offline Client is responsible to secure the generated voting cards against manipulation and encrypting the data in a way that it can only be read by authorized parties. The process of securing voting cards is based on strong cryptographic algorithms:

- **Digital Signature** to confirm the integrity and ownership
- **Authenticated Encryption** to assure the confidentiality and authenticity

The generation and printing of voting cards is carried out at two physically independent locations. At both sites, the processes are carried out in disconnected air-gapped environments. The transfer of voting cards from the sender (generator) to the recipient (printer) requires that the data is cryptographically secured. This document describes the process to ensure the secure transfer of voting cards between sender and recipient:

- **Sender** is responsible to generate and secure voting cards (e.g canton)
- **Recipient** is responsible to verify, decrypt and print voting cards (e.g printing center)

2. Key Exchange

Both parties must exchange key information with their partner so that the cryptographic operations for signature and encryption can be performed. Private key material is never exchanged and remains with the owner at all times. Only public keys are exchanged between the two parties. The responsibilities for both parties are defined as followed:

2.1 Sender

Encryption

- The sender is responsible for the encryption of the voting cards
- The sender uses the public keys provided by the recipient for the encryption process
- The recipient hands over the public keys to the sender in a 4-eyes principle, so that the sender is able to verify the certificates
- The sender checks the fingerprints of all public keys sent by the recipient prior to encryption

Signature

- The sender is responsible for signing the voting cards
- The sender uses his private key for the creation of the signature
- The sender hands over the public key to the recipient in a 4-eyes principle, so that the recipient is able to verify the signature

2.2 Recipient

Signature

- The recipient is responsible for verifying the signature of voting cards
- The recipient verifies the fingerprint of the public key before every signature verification

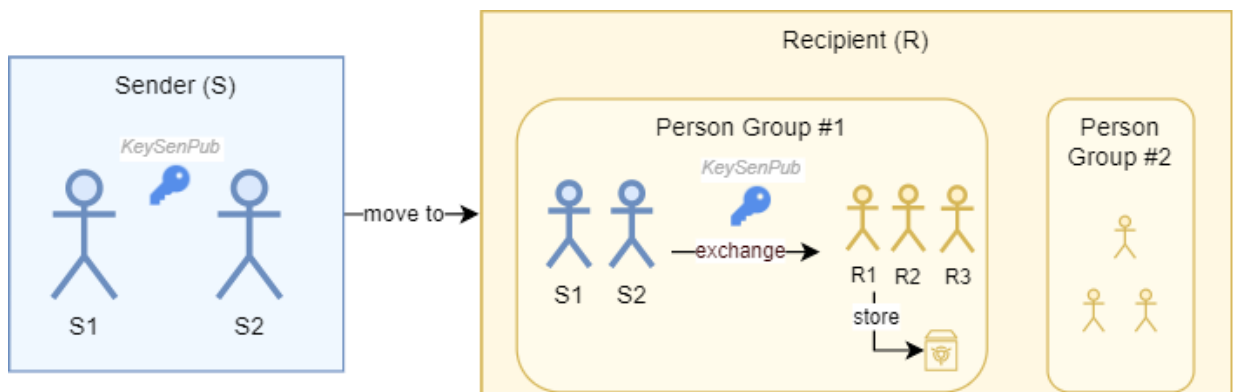
Decryption

- The recipient is responsible for decrypting the voting cards
- The recipient uses his personal PKI card for decryption, which contains the private key

2.3 Signature Key Exchange

The signature public key exchange between the sender and recipient follows a physical exchange to ensure that only trusted keys are used for verifying the signatures.

- The root of trust is defined by human beings and follows a physical exchange process with stakeholders involved from both parties, the recipient and sender.
- The personal identity from each stakeholder involved is physically verified.
- The key exchange involves the following checks:
 - The fingerprint of the public key is calculated and visually verified against a reference fingerprint.
 - The reference fingerprint is provided from a separate physical source from the sender to the recipient.
 - The subject of the public key is visually verified against a reference subject.
 - The public key is securely stored on a USB stick by the recipient and stored in a safe.
 - The public key is only used by the recipient at the time when voting cards are decrypted.








3. Cryptographic Primitives

The process of securing voting cards uses the following cryptographic primitives for various purposes:

Purpose	Cryptographic Primitive	Description
Symmetric Encryption	AES-GCM, 256bit key	The raw data of voting cards is encrypted with a randomly generated AES 256bit key using GCM. It supports block cipher mode with authenticated encryption.
Key Wrapping	RSAES-OAEP-SHA512, 3072bit key	The AES key used for encrypting voting cards is encrypted with each asymmetric key provided by the recipient. Assuming the recipient provides 3 public keys, the same AES key is encrypted (wrapped) 3 times with every public key using asymmetric RSA OAEP with SHA-512. Key wrapping allows 1..n people on the receiving end to have the ability to decrypt the data.
Signature	RSASSA-PSS-SHA512, 2048bit key	The encrypted data including all metadata is signed with the asymmetric private key from the sender using RSA with padding mode PSS and hash algorithm SHA-512.
Sender and Receiver Hash	HMAC-SH256	A salted hash is generated from each encryption and signature certificate's fingerprint (SHA-1) and stored as part of the signed voting card data. On the recipient side the salted hash is used to find the matching certificate by creating the same salted hash from the local available certificates.

3.1 Key Material

	Key Id	Key Owner	Key User	Cryptographic Operation	Key Type	Key Ext.	Key Name (Samples)
	KeyRecPub	Recipient	Sender	Encrypt data	RSA (public)	.pem	voting.encrypted.receiver.cert.pub.pem
	KeySenPriv	Sender	Sender	Create signature	RSA (private)	.p12	voting.signing.sender.cert.p12
	KeySenPub	Sender	Recipient	Verify signature	RSA (public)	.pem	voting.signing.sender.cert.pub.pem
	KeyRecPriv	Recipient	Recipient	Decrypt wrapped key	RSA (private)	.p12	PKI Smartcard (primary) voting.encrypted.receiver.cert.p12 (testing)
	KeySenAes	Sender	Recipient	Decrypt cipher text	AES (secret)	n/a	None (generated at runtime with cryptographically strong random value)

4. File Format

4.1 Conventions

The metalanguage Augmented Backus-Naur form (ABNF) is used to specify the cryptographic process.

- The ABNF syntax follows RFC 5234 and RFC 7405 and references the core rules in RFC 5234, Appendix B.1.
- The base64 encoding used is the standard base64 encoding described in RFC 4648, section 4.
- Refer to: https://en.wikipedia.org/wiki/Augmented_Backus%E2%80%93Naur_form:

4.2 ABNF specification

The following specification defines how voting cards are cryptographically secured. It consists of three main parts:

- The signature from the overall data blob of the voting card
- The header information (HS)
- The encrypted payload

Detailed information of the process steps is defined in chapters encryption and decryption.

```
FILECONTENT      = signature LF content
signature         = 1*base64char ; BASE64(RSASSA-PSS-SHA512(content))
content          = header LF payload
header           = "--- HS" LF version LF sender LF 1*(receiver LF) "--- HE"
version          = 2DIGIT
sender           = "<-" SP sender-salt-enc SP sender-id
sender-id        = 44base64char ; BASE64(HMAC-SHA-256(sender-fingerprint, sender-salt))
sender-fingerprint = 20OCTET
sender-salt-enc  = 24base64char ; BASE64(sender-salt)
sender-salt      = 16OCTET
receiver        = "->" SP receiver-salt-enc SP receiver-id SP receiver-payload LF
receiver-id      = 44base64char ; BASE64(HMAC-SHA-256(receiver-fingerprint, receiver-salt))
receiver-fingerprint = 20OCTET
receiver-salt-enc = 24base64char ; BASE64(receiver-salt)
receiver-salt    = 16OCTET
receiver-payload = 1*base64char ; BASE64(RSAES-OAEP-SHA512(file_key, recipient_pub_key))
payload         = nonce tag ciphertext
nonce           = 12OCTET
tag             = 16OCTET
ciphertext      = 1*OCTET
base64char      = ALPHA / DIGIT / "+" / "/" / "="
```


4.3 Example

Example voting card file with 2 recipients:

```
AAAAAA_(TRUNCATED_VALUE)_AAAAAA==
--- HS
01
<- rgFpU8swZxZErBGVoZS4oA== BBBB (TRUNCATED_VALUE) BBBB==
-> 9YMLmn8DQjabnBYfStlHcA== CCCCCC (TRUNCATED_VALUE) CCCCCC==
-> MxgRiJqt+GhDVZ3M3S16qA== DDDDD (TRUNCATED_VALUE) DDDDD==
--- HE
012345678912AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

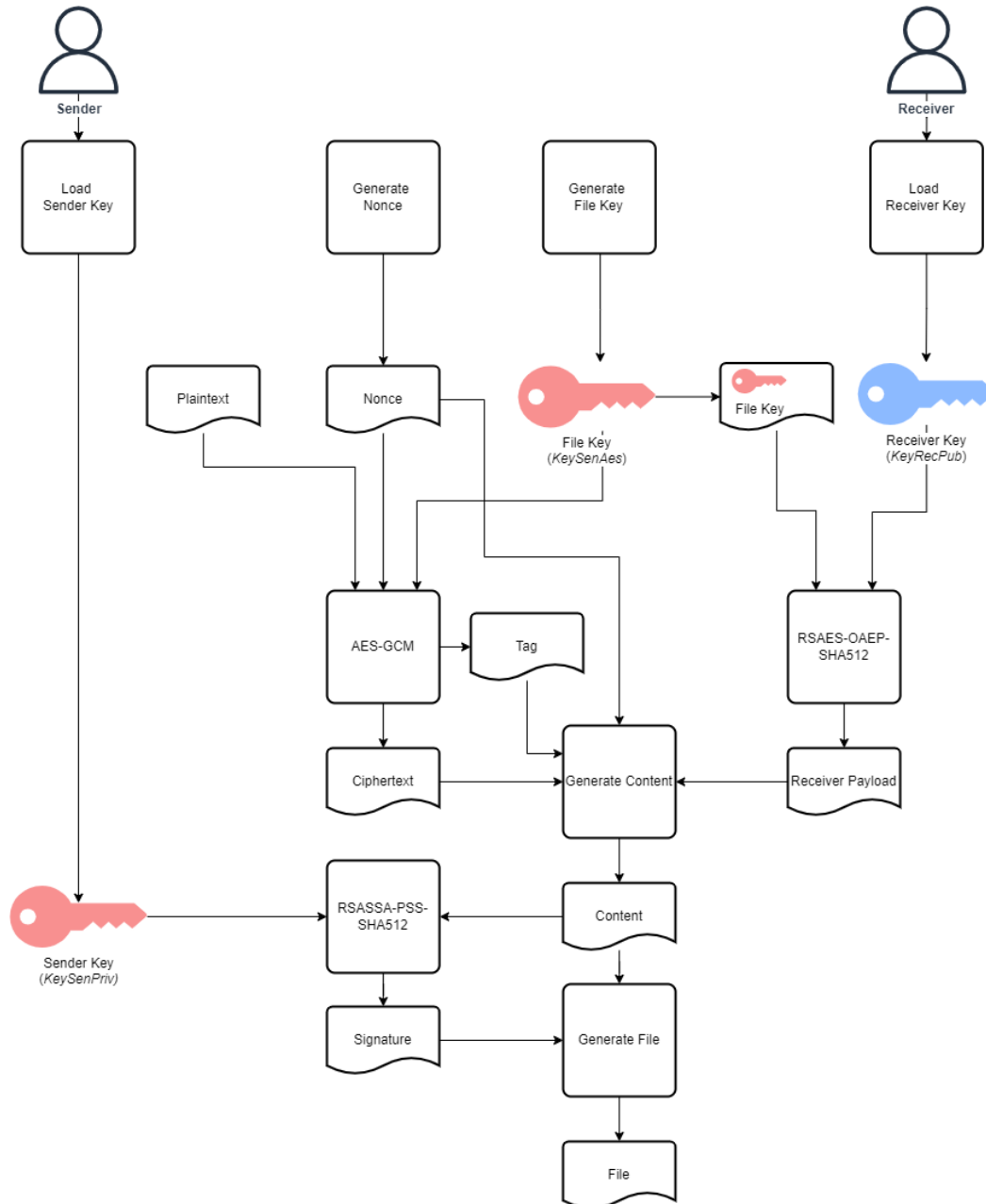
5. Encryption

5.1 Overview

The process of securing voting cards follows a predefined process and follows the cryptographic ABNF specification (bottom-up):



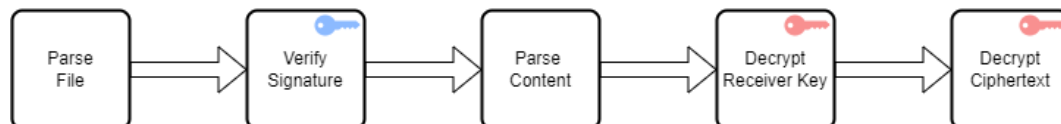
5.2 Detail



6. Decryption

6.1 Overview

The process of decrypting voting cards follows a predefined process and follows the cryptographic ABNF specification (top-down):



6.2 Detail

