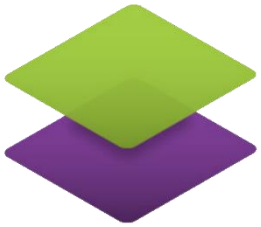


sysmosoft

SENSE Security overview

2014

1 ABSTRACT

The scope of this document is to present the basis of the Sysmosoft SENSE Application security mechanisms and features.

1.1 Out of Scope

The following elements are outside the scope of this document and can be discussed with Sysmosoft upon request:

- Infrastructure Security (Proxies, Firewalls, …)
- Details of cryptography values used by SENSE (IV, salt, iterations, groups, …)

1.2 Sysmosoft Philosophy

Sysmosoft developed the SENSE technology to combat the fundamental shortcomings of infrastructures, mobile devices and third-party components. Unlike conventional products, Sysmosoft implements all security and management mechanisms at the application level with minimal reliance on external components.

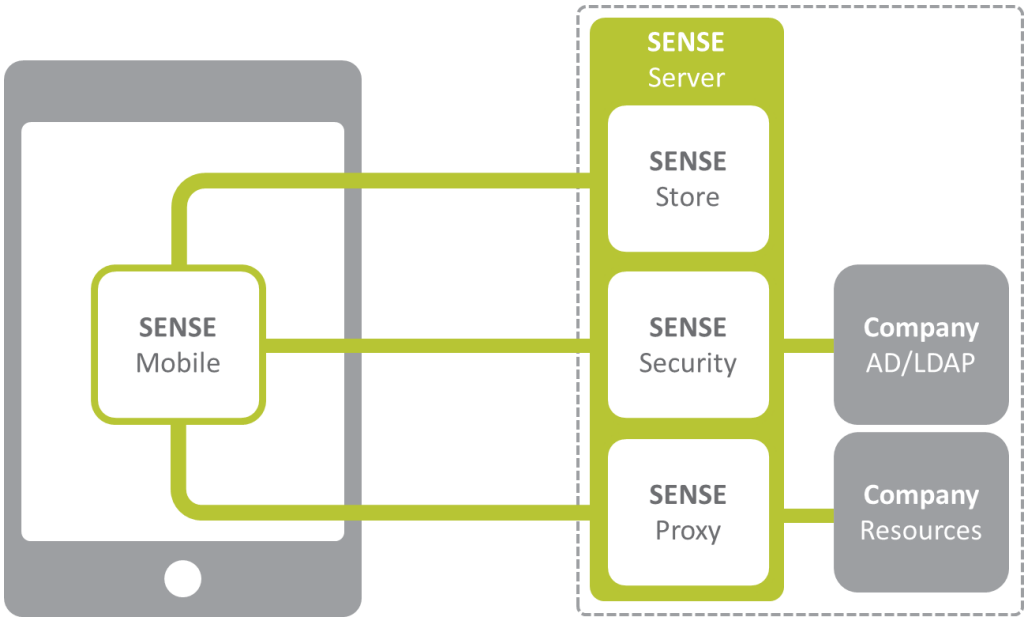
1.3 SENSE Security Mechanisms

- **Key Management:** SENSE generates and manages encryption keys at the application level to avoid using keys provided by untrusted sources
- **Encryption:** SENSE uses state-of-the-art encryption algorithms to encrypt sensitive information at the application level
- **Key Exchange:** SENSE uses key exchange algorithms to generate its own session key between SENSE Server and SENSE Client
- **Strong Authentication:** SENSE uses strong authentication methods to verify the identity of users and devices used to access sensitive data
- **Integrity Control:** SENSE uses strong cryptography algorithms to verify the integrity of sensitive data as well as used applications
- **Authorization:** SENSE verifies user authorization in accessing requested resources prior to allowing access

- **Device Integrity:** SENSE uses advanced preventive features to avoid data leakage due to the risky but user-oriented behaviour of mobile devices
- **Dedicated Cryptographic Libraries:** SENSE uses a dedicated and validated cryptography library to avoid using generic security functions provided by operating systems

2 OVERVIEW

2.1 Schema



2.2 Components

SENSE Mobile: Application deployed within the user's mobile device

SENSE Server: Component deployed within the company network

SENSE Store: Manage mobile application deployment and updates

SENSE Security: Manage groups, users, settings and tasks related to security

SENSE Proxy: Manage access to user's professional data

Company AD/LDAP: Existing company identity server

Company Resources: Existing business data provided by company

2.3 Security Process

1. **Installation:** Install SENSE Mobile on the user's mobile device.
2. **Device Integrity:** Verify that the device complies with company security policy.
3. **Enrolment:** Activate SENSE account for user.
4. **Authentication:** Verify that the user is allowed to access SENSE.
5. **Network Security:** Establish secure connection between SENSE Mobile and Server.
6. **Storage Security:** Establish secure storage on SENSE Mobile.

2.4 Cryptography functions

SENSE uses the following cryptography functions:

Function	
Key agreement	Ephemeral Diffie Hellman
Hash function	SHA-256
Password key derivation function	PBKDF2
Key derivation function	KDF2
Authenticated Encryption Scheme	AES-GCM
Encryption Scheme	AES-CFB
Message Authentication function	HMAC-SHA-256

2.5 Keys Definitions

SENSE uses the following keys:

Key	
Enrolment Code	Value used to activate SENSE on a mobile device
Enrolment Key	Key derived from the Enrolment Code
Authentication key	Key used to verify the identity of the user's mobile device

User Password	Value used to verify the user's identity
Encryption Keys	Set of keys used to encrypt data on the mobile device
Diffie-Hellman Key	Key generated by the Diffie-Hellman key exchange algorithm
Session Key	Key derived from the DH-Key used to encrypt network channel

3 INSTALLATION

Controlling the deployment of mobile applications to users is a challenge for enterprises and typically requires the use of Official Stores located in foreign countries. Unlike generic products, SENSE has embedded deployment mechanisms and includes lifecycle management.

3.1 SENSE Mobile Installation Process

1. Company signs SENSE Mobile using their certificate with Sysmosoft tools
2. Company uploads signed SENSE Mobile to SENSE Store
3. Company provides connection information to out-of-bound mobile users
4. User connects to SENSE Store using his mobile browser (e.g. Safari)
5. User authenticates on SENSE Store
6. User downloads SENSE Mobile as a standard mobile application

3.2 Installation Security

Since the installation process cannot be directly protected by SENSE cryptography, the company defines a deployment process suited to their security requirements. SENSE provides the following security mechanisms during installation:

- **Internal Deployment:** SENSE Store allows companies to deploy their own SENSE Mobile application without having to rely on Official Stores. Access to SENSE Mobile is not public and limited to authorized users.
- **Unique URL Generation:** Users download SENSE using a randomly generated URL by the SENSE Store that is available for a limited period of time. This prevents external parties from downloading SENSE Mobile.

- **Configurable Authentication:** The authentication process to the SENSE Store can be configured to use Company LDAP, a dedicated password, no password or a dedicated method.

4 DEVICE CONTROL

SENSE controls access to critical company information, not the user's mobile device. Devices can become compromised through the actions of the user or by underlying operating system (OS) mechanisms. Risky user behaviors include jailbreaking the device or applying an unsecure configuration. In addition, the OS uses multiple data caches to enhance the user experience, leaking application data to unsecure areas which can be exploited by malicious entities. SENSE combats all these vulnerabilities and more, implementing advanced countermeasures to verify device integrity and prevent data leaks.

4.1 SENSE Device Control Mechanisms

- **OS Conformity Detection:** SENSE detects if a device has been jailbroken or compromised.
- **Anti-debugging:** SENSE detects if an attacker tries to connect to the device and debug the SENSE application.
- **Background Mode Control:** SENSE is able to avoid applications working in the background and wipes the data from the memory once an application is inactive.
- **Pasteboard Cache:** SENSE uses a dedicated pasteboard to ensure that data isn't copied to third-party applications.
- **Keyboard Cache:** SENSE wipes keyboard cache to prevent third-party applications from accessing sensitive text.
- **Device Check:** SENSE checks the device and the OS version to ensure compliance with the company policy.

4.2 Device Control Configuration

SENSE allows companies to define the following device parameters:

- **Set Authorized Device Model:** Define which device model is authorized to access corporate resources

- **Set Authorized Operating System Version:** Define which versions of the OS are allowed to access company resources

5 ENROLMENT PROCESS

Before using SENSE, the user activates their account through the Enrolment Process. The Enrolment Process associates the user with their mobile device by generating a unique Authentication Key shared between SENSE Mobile and SENSE Server. The security of this process is based on state-of-the-art cryptography methods and a one-time password transmitted out-of-bound to the user.

5.1 SENSE Enrolment Process

1. Company activates an Enrolment Process for a specific user
2. SENSE generates a random Enrolment Code for the user
3. Company transmits the Enrolment Code to the user out-of-bound
4. User launches SENSE Mobile Application and enters the following information:
   - Login
   - Password
   - Enrolment Code
5. SENSE Mobile generates Diffie-Hellman request
6. SENSE Mobile computes the Enrolment Key by deriving the Enrolment code using the PBKDF2 function multiple times.
7. SENSE Mobile uses the Enrolment Key to compute a unique message authentication code for the Diffie-Hellman Request through the HMAC algorithm.
8. SENSE Server authenticates the Diffie-Hellman request by verifying the HMAC generated by SENSE Mobile.
9. SENSE Mobile and SENSE Server generate the DH Key.
10. SENSE Mobile and SENSE Server generate the Authentication Key by deriving the DH Key using the KDF2 function.
11. SENSE Mobile and SENSE Server store and protect the Authentication Key

5.2 Enrolment Security

- **State-of-the-Art Key Exchange:** The generation of the Authentication Key is made using the Ephemeral Diffie-Hellman method which allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

- **Authenticated Key Exchange**: SENSE authenticates the Diffie-Hellman key exchange by computing HMAC of requests/responses using a key derived from the Enrolment Code through the PBKDF2 algorithm. The Enrolment Code is generated randomly by SENSE and can only be used once during a specific period.

- **Out-of-bound Initial Secret Exchange:** Preserving the confidentiality of the Enrolment Code is essential in countering middlemen attacks against Diffie-Hellman. For this reason, the transfer of the Enrolment Code from the company to the user is done out-of-bound using a method suited to company security requirements (i.e. phone, letter, fax, email …).

5.3 Enrolment Configuration

SENSE allows companies to define the following enrolment rules:

- **Manual Activation:** Activation of Enrolment is made by the administrator.

- **Enrolment Code Length:** Increasing the length of the enrolment code increases its entropy and improves the overall security level of the Enrolment Process

- **Enrolment Code Duration:** Reducing the validity period of an Enrolment Code reduces the window of opportunity for a potential attacker.

6 AUTHENTICATION

Authentication is one of the biggest mobility weaknesses because mobile devices perform authentications offline and applications typically use weak authentication methods. SENSE employs a dedicated authentication method without impacting user experience or requiring a complex configuration. SENSE also allows adjustments for the best fit with company-specific security requirements. SENSE uses the following authentication factors:

- **User's password**– verified server side using the company identity server (Active Directory, LDAP or other)

- **User's Device**– verified server side by SENSE Server through strong cryptography functions and the Authentication Key
- **Optional Hardware Token**– verified server side by the company authentication server (RADIUS/RSA…).

6.1 Authentication modes

SENSE provides different authentication modes to fit company-specific security and compliance requirements. The following authentication modes can be configured through the SENSE Server:

- **Online authentication:** user identity is verified online by SENSE Server using values stored server side. The online authentication mode provides for maximum security level needs (both user device and password are verified server side).
- **Offline authentication:** user identity is verified offline by SENSE Mobile using values stored on the mobile device. The offline authentication mode provides for reduced security level needs (only the password can be verified and values are stored on the device).

6.2 Online Authentication Process

The SENSE online authentication process is as follows:

1. SENSE Mobile generates a Diffie-Hellman Request to establish an ephemeral session key with the SENSE Server.
2. SENSE Mobile uses the Authentication Key to compute a unique message authentication code of the Diffie-Hellman Request through the HMAC algorithm.
3. SENSE Server authenticates the Diffie-Hellman request by verifying the HMAC generated by the SENSE Mobile.
4. SENSE Mobile and SENSE Server generate the DH Key.
5. SENSE Mobile and SENSE Server establish the Session Key, deriving the DH Key using the KDF2 function and encrypting network communication.
6. SENSE Mobile verifies the user's password through SENSE Server, using the company Identity server (LDAP, AD, other).

7. All authentication factors are validated and SENSE Mobile is authorized to access company resources through the SENSE Server.

6.3 Offline Authentication Process

SENSE Offline Authentication follows the successful online authentication. The offline authentication process is as follows:

1. User launches SENSE Mobile and enters their password.
2. SENSE Mobile computes the Local Authentication Key by deriving the user's password several times through the PBKDF2 function.
3. SENSE Mobile completes the process authentication by verifying computed Local Authentication Key with the reference Local Authentication Key.

6.4 Authentication Security

- **Online Strong Authentication:** SENSE's strong authentication method is based on state-of-the-art cryptography techniques. By combining the Authentication Key and the user's password, SENSE can verify the identity of the user and the mobile device and establish a secure communication channel between the SENSE Server and SENSE Mobile.
- **Online Mutual Authentication:** The SENSE Server Environment and the SENSE Mobile Environment mutually authenticate each other. Unlike the case with a simple server authentication, an attacker cannot steal the identity of one of two elements without access to the Authentication Key. The Authentication Key is stored within the organization and protected on the user's mobile device.
- **Online Authentication Check:** Performing SENSE authentication online provides control over the number of failed attempts allowed and the blocking of a user account to prevent brute force attacks. Compared to standard offline checks, performing this process server side ensures attackers are not able to bypass the maximum number of attempts.
- **Cryptographic Camouflage**: SENSE can be configured to encrypt the Authentication Key on the device using a "Cryptographic Camouflage" technique. The Authentication Key (pure random bits) is encrypted using the AES-CFB algorithm and a key derived from the user's password through the PBKDF2 algorithm. To further defend against brute force attacks, only the result of the encryption is stored on the device and no checksum or

information verifying a successful decryption is stored. The only verification of decryption is through the server, which limits the number failed attempts.

- **Offline Best Practices:** When performing authentication offline, SENSE uses PBKDF2 with a large number of iterations to generate a key from the user's password. This best practice aims to significantly increase the time taken for attackers to obtain a password offline.

6.5 Authentication Configuration

SENSE allows companies to define the following authentication parameters:

- **Authentication Key Validity:** Defines the validity duration of an Authentication Key and when a new one will be generated.
- **Maximum Authentication Tries:** Defines how many times an incorrect password can be entered on the mobile device.
- **User Inactivity Timeout:** Time period during which the user does not interact with SENSE. After this period SENSE automatically locks access without cleaning the memory.
- **Session Inactivity Timeout:** Time period during which SENSE does not communicate with the Server. After this delay the Session is closed and the memory is cleaned.

7 NETWORK PROTECTION

Mobile devices are by nature used everywhere and therefore susceptible to unsecure network connections. Through these untrusted network connections, attackers execute middlemen attacks to access sensitive data and break into the company network. SENSE establishes a dedicated secure channel between SENSE Mobile and SENSE Server to protect the confidentiality and integrity of company data.

7.1 Network Request Process

Once the online authentication is performed, SENSE uses the following process to send business requests from SENSE Mobile to SENSE Server:

1. Session Key established during 6.2 Online Authentication Process
2. SENSE Mobile generates new business request

3. SENSE Mobile encrypts requests using AES-GCM algorithm with the Session Key
4. SENSE Mobile sends encrypted request to SENSE Proxy
5. SENSE Proxy requests SENSE Security to verify request's authorization and deliver related Session Key
6. SENSE Proxy decrypts and authenticates requests using AES-GCM algorithm with Session Key
7. SENSE Proxy execute the business request on the server side

7.2 Network Security

To mitigate OS security limitations and network security configuration vulnerabilities, SENSE integrates the following security features at the applicative level:

- **Standard SSL/TLS Security:** By default, SENSE establishes a HTTPS secure channel between the SENSE Mobile and the SENSE Server using best practices. The HTTPS is used in server authentication mode with the cipher suite supported by the company HTTPS proxy.
- **Data Encryption and Authenticity Control:** All data exchanged between SENSE device and SENSE server are encrypted and authenticated through the AES-GCM algorithm. An attacker will not be able to read or modify content without having access to the key generated with the Diffie-Hellman algorithm.
- **Perfect-Forward-Secrecy:** The Session Key is generated using Diffie-Hellman key exchange algorithms, establishing keys in a strictly confidential manner. Furthermore, even if an attacker were to trace the encrypted communication and access a key, they would still be unable to decipher the archived data.

7.3 Network Configuration

- **Session Key Duration:** Define the validity period of the Session Key prior to forcing the generation of a new key

8 LOCAL STORAGE

SENSE protects company data at rest on the mobile device by offering advanced encryption, dedicated key management and advanced storage policy. Protecting local data at the application

level avoids reliance on the native device security. This ensures that keys and cryptographic algorithms used are completely independent from the one used by other personal and potentially malicious applications.

8.1 Local Storage Modes – Key Management

SENSE provides advanced storage modes to cater to company specific security or compliance requirements. The following storages modes can be configured on the SENSE Server:

- **No Data Storage:** SENSE can deactivate data storage on the user's mobile device. In this mode, the device acts as a simple terminal which only allows visual access to the information. Once the task is completed, the memory is erased and no trace of the data is left.

- **Online Storage:** In the online storage mode, data is encrypted by SENSE using the authentication-encryption algorithm AES-GCM. The Encryption Keys used to encrypt local data are generated server side and transmitted to the device after authentication. Once the user's session is terminated, Encryption Keys in memory are wiped. As such, local data cannot be accessed when a device is lost or stolen.

- **Offline Storage:** In the offline storage, data is also encrypted by SENSE using the authentication encryption algorithm AES-GCM. The Encryption Keys used to encrypt local data are encrypted on the mobile device using a key derived from the user's password. The encryption strength is based on the complexity of the user's password.

8.2 Local Storage Security

SENSE provides the following principal security features to protect local data:

- **Native Encryption:** SENSE uses native device encryption and best practices (keychain, Secure APIs …) to store sensitive data on the mobile device.

- **Application Level Authenticated Encryption:** In addition to standard device security, SENSE Encrypts data at the application level using the AES-GCM authenticated encryption. This second encryption layer ensures sensitive data stored locally remains inaccessible even when the first layer of device encryption is compromised.

- **Dedicated Key Management:** Companies have full control over encryption keys and decide where they are stored (server side or on the mobile device). Keys used by SENSE are independent from the ones provided by the operating system or used by third-party

applications. Data is therefore encrypted with keys not accessible by unauthorized entities or personal applications.

- **Key Wipe:** When Online Storage is activated, encryption keys are stored server side and can therefore be easily wiped when a device is lost or stolen. In contrast to traditional solutions that wipe unencrypted data on the device, SENSE key wipe mechanisms ensure that any data remaining on lost or stolen devices cannot be compromised by potential attackers because the key is not accessible.

- **Strong Keys:** SENSE generates strong 256 bit Encryption Keys server side. Using strong keys protects local data against brute force attacks, especially if the keys are stored server side.

8.3 Local storage configuration

SENSE allows companies to define the following parameters:

- **Local Cache:** Allow or prevent data storage on the mobile device.

- **Enable/Disable Offline Access:** Allow or prevent users from accessing data when the network connection is unavailable.

- **Define Encryption Key Validity:** Defines the validity period of Encryption Keys and when the new one will be automatically generated by SENSE.

- **Define Offline Access Validity:** Defines the period during which the user can access data offline. After this period an online connection shall be executed.

9 CONCLUSION

Sysmosoft SENSE is a highly secured Swiss mobile solution that enables increased workforce productivity and embraces mobility challenges without compromising sensitive company data or the user's personal experience. By implementing security and management mechanisms at the application level, SENSE enables you to surpass the limitations of the device and reduce reliance on external components to leverage secure mobility in your organization.

For more information on Sysmosoft SENSE technology or product solutions, please contact us on the company website www.sysmosoft.com or by email at info@sysmosoft.com.