SONY

Xperia™ in Business

Security

Read about how Xperia devices manage security
in a corporate IT environment

April 2016

XPERIA

About this document

Products covered

This document describes Xperia in Business enterprise services and features in Sony Mobile devices. Please refer to the tables in the Product overview document for details about supported products and software versions.

Note: xxx in software versions denotes the number “001-999”.

To find the software version of a device, select **About phone** in **Settings**.

Limitations to services and features

Some of the services and features described in this document might not be supported in all countries/regions or by all networks and/or service providers in all areas. Please contact your network operator or service provider to determine availability of any specific service or feature and whether additional access or usage fees apply.

Trademarks and acknowledgements

All product and company names mentioned herein are the trademarks or registered trademarks of their respective owners. Any rights not expressly granted herein are reserved. All other trademarks are property of their respective owners.

Visit www.sonymobile.com for more information.

Document release date

April 1, 2016

This White paper is published by:

Sony Mobile Communications Inc.,
4-12-3 Higashi-Shinagawa, Shinagawa-ku,
Tokyo, 140-0002, Japan

www.sonymobile.com

First released version (April 2016)

Table of contents

Xperia devices offer a robust security architecture to secure communications and to protect data stored on the device. The Android™ security model combines with Sony Mobile enhancements to provide a stable and secure platform.

Robust architecture with multiple layers

Xperia devices from Sony provide a multi-layer security architecture:

- **System security** - Xperia devices offer Linux kernel-level security from Android™ with Sony Mobile enhancements like Runtime integrity, HW and SW integrity and Secure Boot Chain.
- **Secure storage** - Devices can be protected by passwords, PIN codes, fingerprints and screen unlock patterns. Data on the devices can be encrypted.
- **Network security** - Transmissions are encrypted and Xperia devices have built-in support for industry-standard VPN protocols.
- **Device security** - Administrators can control the use of certain features or apps on devices. Data from lost devices can be wiped.
- **Digital certificates** - Xperia devices support digital certificates to enable authentication and authorisation of users connecting to corporate networks.

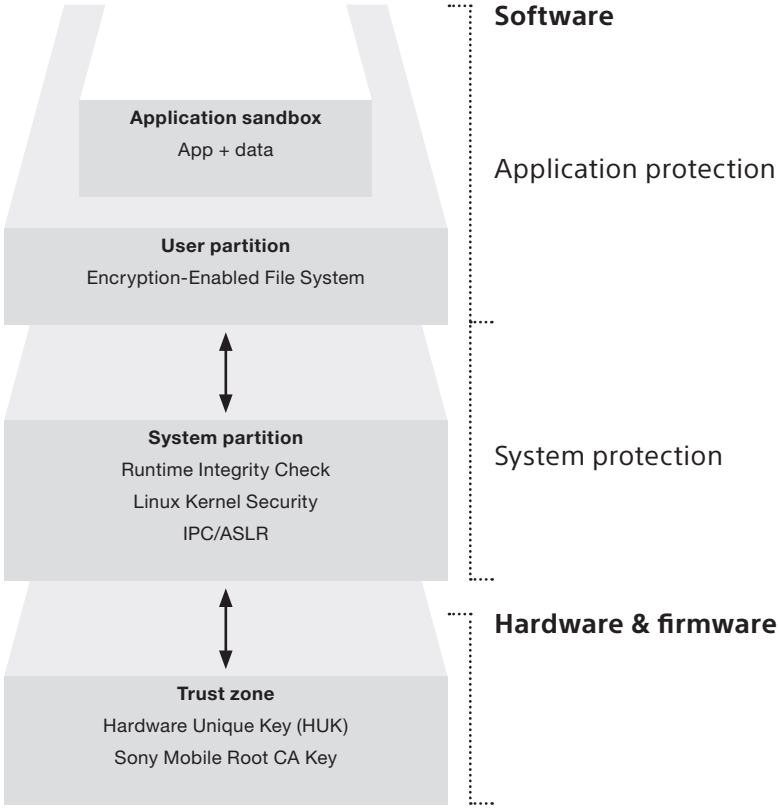

Figure 1: Xperia™ system security

System security

The Android operating system offers a well-defined security architecture. As the Android OS is based on the Linux™ operating system, it takes advantage of the proven Linux kernel-level security model. The OS uses the Android Application Sandbox, which isolates application data and code execution from other applications. Since applications cannot interact with each other, and have limited access to the OS, sensitive information is protected if the user doesn't permit access.

System security in Xperia devices from Sony:

- SE Linux, enforcing mode
- Application sandbox
- Application code signing
- User-based permissions for applications
- Interprocess Communication framework
- Malware scanning of apps
- Address space layout randomiser
- Secure boot chain
- Runtime integrity check

Linux kernel security

The Android OS is built upon the Linux kernel. The Linux kernel has been developed and improved constantly for over 20 years, and it is used and trusted as a stable and secure kernel by many corporations and security professionals. Android uses Security Enhanced (SE) Linux access control in enforcing mode.

Application sandbox

The Application Sandbox in the OS kernel protects native code and OS applications. All software above the kernel, including libraries, application runtime and applications, runs inside the Application Sandbox. The fact that the Android platform does not allow applications on the device to interact with each other and limits their access to the OS is key to enforcing security in Android devices. This system is referred to as the Android Application Sandbox. The Android OS assigns a unique Linux user ID to each application. The application then runs as a unique Linux user in a separate process. This means that if one application tries to read data or start a process in another application without permission, this action is stopped by the OS since the instigating application doesn't have the appropriate user privileges.

Application code signing

Each application that is used in the Application Sandbox on an Android device must be signed. Without a legitimate signature, an application cannot be installed; it will get rejected by either Google Play™ or by the package installer on the Android device. The certificate of the signed application defines the user ID that is associated with that application. Application signing also ensures that one application cannot access any other application except through well-defined inter-process communication (IPC). In addition, apps available from Google Play are automatically scanned for malware.

User-based permissions for applications

Without a user's explicit permission, an Android application cannot access any system resources or sensitive APIs, with a few limited exceptions. Trusted applications can use sensitive APIs, but only after the user has given permission. Examples of sensitive APIs are camera functions; location data (GPS); Bluetooth and NFC wireless technologies; telephony functions; SMS and MMS functions; and network and data connections. These API resources are only accessible through the OS. To be able to use a sensitive API on the device, an application must state which capabilities it needs. When an Android application wants to use a sensitive capability for the first time, you must decide whether you want to approve the permissions that the application requests. It is also easy to turn on and off permissions at a later stage for individual apps that want to use a certain capability.

Protected APIs that cannot be accessed without a user's explicit permission include:

- Camera functions
- Location data (GPS)
- Bluetooth® and NFC functions
- Telephony functions
- SMS/MMS functions
- Network/data connections

Interprocess communication

The Android OS uses Linux interprocess communication (IPC). It is a well-defined and proven framework for how multiple processes are allowed to communicate with each other. The Linux IPC mechanism has been developed and tested for decades.

Malware scanning of apps

An important element in the security shield provided by the Android platform is the distribution of secure apps. The server-side scanner, Google Bouncer, controls each app to verify that its signature does not match that of known malware. When a developer uploads an app to Google Play, it is automatically scanned. The app is then scanned at regular intervals.

Users can also choose to enable "Verify Apps" and have their devices regularly checked for malware. App verification can alert the user if they try to install an app that might be harmful; if an application is especially bad, it can block installation.

Address space layout randomiser

The task of the Address Space Layout Randomiser (ASLR) is to make sure that system applications and libraries are stored in random locations in the memory. The Android OS uses this randomisation to protect the device against exploitation of the memory, and against malware getting installed on the device with the risk of corrupting the memory. ASLR prevents Return-Oriented Programming (ROP) attacks. Most binaries are randomised when executed because they are linked with the PIE (Position Independent Executable) flag. The linkers are randomised in the process address space. The Android OS has full stack, heap/brk, lib/mmap, linker, and executable ASLR.

Sony Mobile secure boot chain

Each step of the boot-up and the software update processes contains components that are cryptographically signed by Sony to ensure integrity. The processes proceed only after the chain of trust is verified. This includes the bootloaders, the kernel and the modem firmware. When an Xperia device is started, its application processor immediately executes code from a read-only memory known as the Boot ROM. This unchangeable, permanent code is entered in the chip as part of the manufacturing process, and is implicitly trusted.

The Boot ROM code contains the Sony Root CA public key, which is used to verify that the Sony S1 bootloader is signed by Sony before it is allowed to load and run. This is the first step in the chain of trust where each step ensures that the next is signed by Sony. When the S1 bootloader finishes its tasks, it verifies and runs the Android OS, i.e. the Linux kernel. When you update the software on your Xperia device, either by using a USB cable and a computer, or by updating directly in the device, over the air, all updates are signed by Sony.

This means that all software is verified at least twice: once when it is written to the device, and then every time the device is turned on. This secure boot chain ensures that the lowest levels of the software are not tampered with. If one step of this boot process is unable to load or verify the next step, boot-up is stopped and the device turns off. To be able to start and use the device again, you have to restore it by updating the software using a USB cable and Sony Mobile's computer tool, Xperia Companion.

Runtime integrity check

To further improve security in Xperia devices, Sony has introduced a runtime integrity check to detect runtime attacks. The runtime integrity check is integrated in the kernel and verifies that the mount table has not been modified. This is to prevent attackers from, for example, storing executables that remount and modify the system partition of the memory to make root access permanent.

Secure storage

Xperia devices provide proven methods for protecting sensitive information. Passwords, PIN codes, screen unlock patterns and, for some devices, fingerprint sensors help prevent unauthorised use. Data on the device can be encrypted, making the data unreadable to anyone but the intended user. The combined efforts of a strong password and encryption capabilities guarantee robust protection of sensitive data stored on Xperia devices, and a lost device can be remotely locked and wiped to protect sensitive content.

Encryption

Encryption can be activated in Xperia devices. Xperia devices offer full encryption with 256-bit AES for all user data in the internal memory, as well as any external SD™ card. This means that any data saved by and to applications, for example, email messages, email attachments, text and multimedia messages and contacts, is protected with a hardware encryption key against unauthorised access. A phone that ends up in the wrong hands does not risk having its file system broken into.

All data is encrypted by a key derived from the user password or PIN. If a device gets lost, confidential corporate information stays safe, and can only be accessed by knowing the password. To strengthen protection and guard the device against systematic password guessing attacks, the password is combined with a random salt and hashed repeatedly with SHA1 using the standard PBKDF2 algorithm prior to being used to encrypt the file system key.

In addition, Xperia devices can defend themselves from dictionary password attacks by enforcing password complexity based on rules that your IT department can set. On Xperia devices, encryption can be enforced by an organisation's IT department through Microsoft® Exchange ActiveSync® (EAS), Enterprise Mobility Management (EMM) or Mobile Device Management (MDM). Encryption can also be activated on the device by the user.

The email application in Xperia devices can use SSL and TLS to encrypt data sent between the Android OS and corporate services. To further enhance security in email conversations, the Xperia email application offers S/MIME (Secure/Multipurpose Internet Mail Extensions). This protocol gives Xperia devices the possibility to view and send encrypted email messages. It can also be used to prevent users from moving email messages between accounts and from forwarding messages from an account other than the one that received them.

Secure email S/MIME In EAS and the native Email client:

- SHA-1/SHA-256*
- Triple-DES, AES 128/192/256-bit*

*Only SHA-1 and Triple-DES support if S/MIME policies are enforced through EAS.

S/MIME policies supported by the Xperia Email application:

- Require signed S/MIME messages
- Require encrypted S/MIME messages
- Require signed S/MIME algorithm
- Require encryption S/MIME algorithm

FIPS 140-2 certification

The FIPS 140-2 (Federal Information Processing Standards) standard is a security accreditation program for cryptographic modules used to handle sensitive information. With the FIPS 140-2 certification, supported Xperia devices can be included in enterprise and carrier short lists for devices that fulfill mandatory security requirements at the highest level.

Common Criteria certification

Sony Mobile has initiated a Common Criteria (CC) evaluation of some devices that claim conformance to Protection Profile for Mobile Device Fundamentals (MDFPP) version 2.0. Sony Mobile is cooperating with atsec, a government-accredited Common Criteria testing laboratory in Sweden, Germany and the United States. The certification will be carried with CSEC - Sweden's national certification body for IT security in products and systems according to the standard Common Criteria. The Common Criteria and the internally-recognised ISO standard (ISO/IEC 15408) are used by governments and other organisations to assess security and assurance of information technology products. The Common Criteria standard provides a uniform way of expressing security requirements and defines a set of criteria by which a product's security aspects can be evaluated.

Data protection

The combination of a strong password and 256-bit AES software encryption creates a robust encryption key that safeguards corporate data. This setup hinders data from becoming available to unauthorised users when the device is locked, and helps keep device content secure even if the device comes under virtual or physical attack. To activate data encryption, the user simply has to set up password protection from the Settings menu on the device. A strong password is recommended to ensure effective data protection. IT departments can enforce strong passwords using Microsoft® Exchange ActiveSync® or MDM solutions.

Remote wipe

On an Xperia device that gets lost, stolen, or otherwise compromised, the administrator can remotely remove all data from the device and deactivate it. This remote wipe procedure can be performed using the Exchange Management Console (Exchange Server 2010 and later) or Exchange ActiveSync Mobile Administration Web Tool (Exchange Server 2003 or 2007). Users can wipe their devices remotely themselves using Outlook Web Access if they use Exchange Server 2007. Xperia devices can also be remotely wiped using third party EMM/MDM solutions or the 'my Xperia' service, even in situations where an Exchange server is not used.

Local wipe

Xperia devices can be set up to wipe all data and shut down after a set number of failed login attempts. This ability, known as local wipe, makes sure that brute force cracking attempts are unsuccessful. The number of failed attempts allowed before a local wipe occurs can be set in a configuration profile using EMM/MDM, or by using Microsoft® Exchange ActiveSync® policies enforced over the air.

Secure and local storage of information with software from Sony

Small- and medium-sized companies that don't want to rely on Microsoft® Exchange ActiveSync® or EMM/MDM solutions for synchronisation and remote storage of information can use free-of-charge software from Sony Mobile that is made for Microsoft® Windows® and Mac OS® computers. This tool can be used to back up and restore data locally on a computer. There is no need to create accounts or access the Internet.

Tools for Microsoft® Windows® and Mac OS® users

Xperia Companion is a software application for Microsoft® Windows® 7 and higher, and for Mac OS® X 10.8 and higher. It offers local backup and restore functions. When the Xperia Companion software is installed on a computer, users simply connect their Xperia device to the computer using a USB cable. If needed, all necessary drivers for the connected Xperia device are installed by Xperia Companion. Xperia Companion features software update and software repair functionality, enabling Xperia devices to be kept up to date and to run smoothly. Users can also use the tool to browse content in their devices, using a USB cable.

Xperia Companion is available for free download at www.sonymobile.com. The Backup & Restore function supports the backup of the call log as well as contacts stored locally on the device memory. Users can also back up text messages, bookmarks, system settings, application settings, data (availability depends on the application) and media files. The backup and restore procedure is performed between the Xperia device and the computer or a local server, that is, using a local connection that does not require Internet access.

The Backup & Restore feature in Xperia Companion supports:

- Backup of the call log and contacts stored locally in the phone memory
- Backup of text messages, bookmarks, system settings, application settings and data (availability depending on application)
- Media files

Network security

Xperia users within businesses and various organisations expect to be able to access corporate networks wherever they are. At the same time, they require that their data is protected over a reliable connection, with robust user-authorising methods in place. Xperia devices based on the Android OS meet these security requirements whether users are connected via a mobile network or a Wi-Fi connection.

Using tethering, an Xperia device can also be turned into a mobile hotspot to access the Internet safely from a computer. In the corporate environment different network access methods and levels can be set to match corporate IT policies, depending on where the device is used and which tools are available.

Secure connections

To encrypt communication between Xperia devices and corporate services, Xperia devices use the following security standards: Secure Socket Layer (SSL) 2.0 and 3.0, and Transport Layer Security (TLS v1.0, v1.1 and v1.2). Internet-based applications, such as the web browser, Email application and the Calendar, use SSL/TLS to encrypt information sent over the Internet. There is also support for StartTLS with IMAP/POP3 accounts.

Encryption of email and other data in transmission supported by Xperia devices from Sony:

- Secure Sockets Layer (SSL) version 2.0 and 3.0
- Transport Layer Security (TLS) versions 1.0, 1.1, and 1.2
- StartTLS (with IMAP/POP3 accounts)

Virtual private network (VPN)

Xperia users can connect to a corporate network with VPN access by using industry-standard protocols and user authentication. Xperia devices and the Android OS support several VPN technologies, which makes the integration of Xperia devices into an existing VPN solution easy. Compatibility with a wide selection of VPN technologies combined with the Xperia device support for user authentication using the X.509 Digital Certificate Standard results in robust protection for all remote connections. Xperia devices support clients using standard Android APIs from leading VPN solution providers such as Cisco and Juniper.

VPN protocols supported by Xperia devices from Sony:

- PPTP with PPP encryption (MPPE)
- L2TP/IPSec PSK/RSA
- IPSec Xauth PSK/RSA
- IPSec Hybrid RSA
- SSL VPN (available through third party applications)

VPN features supported by Xperia devices from Sony:

- API for VPN solutions from leading vendors certificate-based authentication support
- Always-On VPN
- VPN per user on multi-user devices (tablets only)

Wi-Fi®

To provide the highest level of protection for data transmissions over a Wi-Fi connection, Xperia devices use WPA2 Enterprise with 128-bit AES encryption. In addition to the encryption, protection is enhanced by requiring authentication for access to a wireless network. X.509 digital client certificates authenticate a user as a valid user before permitting access to the network. Xperia devices also support 802.1x wireless authentication methods, which means that they can be used with numerous RADIUS authentication solutions.

To enable easy setup when connecting to Wi-Fi networks, Xperia devices support Wi-Fi Protected Setup™. Xperia devices can be set to automatically connect to Wi-Fi networks within range. Once set up, networks that require login credentials or other information are quickly accessed via automatic identification and web browser support. Once login credentials have been entered, they are reapplied when needed as long as the original login window in the web browser is kept in the background. In addition, Xperia devices support roaming based on the RSSI (Received Signal Strength Indicator) level, which improves the Wi-Fi connection and authentication for devices moving between access points. RSSI-level roaming improves connection reliability by automatically switching from an access point with a weakening signal to a neighbouring access point with a stronger signal.

Xperia devices support Wi-Fi connections to internal or external network resources via a proxy server. To enhance the battery life in Xperia devices, users can set Wi-Fi to be turned off when a device is out of range of known access points. In order to reduce power consumption in idle mode, Xperia devices support WMM® Power Save and IEEE-PS.

Wireless authentication methods supported by Xperia devices from Sony:

Industry-standard security protocols

- WAPI (for China)
- WEP
- WPA/WPA2 Personal
- WPA/WPA2 Enterprise

802.1x authentication methods

- EAP-SIM
- EAP-AKA
- EAP-TLS
- EAP-TTLS
- EAP-PWD
- PEAPv0 (EAP-MSCHAPv2)
- PEAPv1 (EAP-GTC)

Certificate-based authentication support

Proxy support

Wi-Fi Protected Setup (WPS)

Bluetooth™

Xperia devices have support for Bluetooth version 4.2, which enables secure connections to other devices, like computers, tablets, phones, printers or headsets, supported by Bluetooth technology. Xperia devices supply faster data transfer with Enhanced Data Rate (EDR) and they also have support for Secure Simple Pairing (SSP), enabling Public Key Infrastructure (PKI) encryption that protects against Man-in-the-middle (MITM) eavesdropping attacks and safeguards the integrity of the communication.

Enterprise single sign on

Enterprise single sign on (SSO) enables user credentials to be used across apps. Each new app configured with SSO verifies user permissions for enterprise resources, and logs users in without the need to reenter passwords. The SSO solution used in Xperia devices is Kerberos compliant and uses Active Directory verification.

Device security

The screen lock combined with a passcode (a PIN or an alphanumeric password) or a fingerprint is the first security barrier in preventing unauthorised users from gaining access to the entire device. It protects business as well as personal information. The passcode can be set by the user or enforced by the IT department. The complexity of the password and other password-related requirements can be configured and enforced via EMM/MDM or Microsoft® Exchange ActiveSync® policies over the air. In addition to enforcing passcode policies, the use of device management solutions with Xperia devices enables you to control device policies and device administration features. For example, you can restrict the use of certain features or apps on devices, or wipe data from lost devices.

Passcode policies

IT administrators can choose from a wide range of passcode requirements when deploying Xperia devices in a corporate environment. In addition to requiring that an Xperia device is supplied with a passcode, you can enforce what length a PIN or a password must have through the Minimum password length policy. By using the Restrict password history policy, you can force users to create a new passcode that is different from their current passcode or a recently used passcode. This policy is often combined with the Password expiration timeout policy which forces users to update their passcode after a specified time period.

Device policies and administration

For an even higher level of security, you can add policies restricting the use of certain features on a device, or determine which features should be disabled or enabled. Security policies developed by Sony Mobile for Xperia devices include encryption of the external SD card. This is an addition to the Android OS support for device policies. You can, for instance, require that the storage of the device has to be encrypted, or that the camera should be disabled.

Xperia devices also support application blacklists and whitelists. This feature allows third party EMMs (Enterprise Mobility Management) and MDMs (Mobile Device Management) solutions to add and remove applications to the lists. Applications on the blacklist are disabled, and if they are started the user will get a notification that says that the application is blocked due to device policies.

Within the device administration area, the Android OS provides a toolbox of administration features, ranging from the possibility to remotely lock a device and wipe its content (including the content on the external SD card) all the way through to remotely installing applications and updating installed applications.

Enforcing policies

By using device management solutions, an IT administrator can reach the whole fleet of Xperia devices used in a company. By managing devices from one central point, you can guarantee a high level of security by being able to enforce and monitor a wide range of parameters in the devices that access your corporate network and its sensitive data. You can achieve a comprehensive security setup as all devices in your network follow the same set of rules. You can configure different rule sets based on different user types.

When using Xperia devices, you can take advantage of the policies added by Sony Mobile as well as standard policies supported by the Android OS. You can remotely configure password settings, and push out policies to Xperia devices over the air using MDM solutions that support standard Android APIs. If the Xperia device uses a Microsoft Exchange account, you can push Microsoft® Exchange ActiveSync® policies over a mobile or Wi-Fi network.

Fingerprint sensor

Some Xperia devices are equipped with a fingerprint sensor. You can use it to unlock screen lock protection and for online payments, using the FIDO standard. The fingerprint sensor and the fingerprint image is only accessible from a secure driver running in TrustZone. This means that even if the Android OS is compromised, the security of your fingerprint image is not compromised.

The fingerprint sensor in Xperia devices is a capacitive scanner that uses an array of capacitive proximity sensors to create a digital image of a human fingerprint. Instead of photographing an image of the ridges and valleys in a fingerprint as an optical scanner does, a capacitive scanner's sensors generate a complex pattern of electrical currents, which are processed to form a digital image of the fingerprint. Since the capacitive scanner requires the physical presence of a human finger in order to generate the image, it is more secure than an optical device.

My Xperia Theft Protection and Google Factory Reset Protection

By enabling the My Xperia Theft Protection service or Google Factory Reset Protection you can set up your Xperia device to prevent other people from using it if it's been reset to factory settings without your permission. If your device is wiped – for example by performing a software repair using Xperia Companion – a protective mode called Lockdown will be activated and only someone with your Google account credentials can use the device.

In Lockdown mode the device will be completely useless:

- All running applications are stopped.
- You can no longer maximise the notification panel.
- Incoming calls are sent to voicemail (if available).
- Outgoing calls (except emergency calls) are blocked.
- The USB port will only be available for charging. It will not be possible for a PC or Mac to detect the device. This also applies to a software repair or flash.

Lockdown will remain in effect until the user has validated the device using the correct Google credentials. Reloading software or rebooting the device will not disable the service.

Digital certificates

Xperia devices support digital certificates, providing businesses and organisations with a way to authenticate and authorise users to securely and efficiently transfer information to and from corporate networks. In addition, digital certificates enable the encryption of data exchanged between servers and permitted devices. The security is built around the Public Key Infrastructure (PKI) framework, which uses trusted encryption keys to protect transmitted data.

Certificates are issued and approved by a Certificate Authority (CA). The CA could be an independent external company which is recognised and mutually trusted, or an internal organisation within your business. Digital certificates can also authenticate a client or a device interacting with a network, attesting that the device really is the device that it claims to be. Moreover, certificates are used to verify the sender of, for example, email messages or documents, with the option of making sure the content is encrypted.

Server certificates

Xperia devices support client-server communication using Transport Layer Security (TLS) or Secure Socket Layer (SSL). Authentication with server certificates follows the X.509 digital certificate standard. Server certificates are stored in the internal credential storage. Server certificates enable encrypted communication between the client and the server.

Client certificates

You can use client certificates as an efficient alternative to authentication by requiring a user name and password, or a token. EAS servers, VPN gateways or Wi-Fi access points can identify Xperia devices using client certificates before giving them access to a corporate network. In this setup, users must obtain and store the certificate on the Xperia device before they can configure the device to use a VPN gateway or a corporate server. Client certificates may also be used to enable secure messaging using S/MIME. Client certificates are stored in the secure credential storage and protected by a user-selected password.

Client and CA (Certificate Authority) certificates:

- X.509 standard based
  - DER encoded (*.crt, *.cer)
  - PKCS#12 key store files (*.p12, *.pfx)
- Stored in trusted credentials storage
- Installed from several sources:
  - SD card
  - Email
  - Web browser
  - MDM provider

Certificate-based authentication support in multiple apps

- Exchange ActiveSync (EAS)
- Wi-Fi
- VPN
- Web browser
- Other third party apps

Certificate Pinning

- Protection against compromised Certificate Authorities

Installing or removing digital certificates

When opened, a PKCS#12 keystore file triggers the KeyChain installer, which installs a bundled private key/certificate pair. IT administrators can distribute certificates by making the required files available for download from a secure server area to the SD card. The user can then install the files on the device from the SD card.

Certificates can also be distributed via email, since the email application allows the installation of certificate files directly from an attachment. In such cases, you can simply attach the files in an email and then let the user install the files by opening them. Alternatively, several browsers support the installation of digital certificates. So users can download the certificate files from a secure corporate website to the Xperia device.

You can also distribute digital certificates over the air through an existing EMM or MDM solution. You can remove an installed certificate via the Settings menu in the Xperia device. Alternatively, you may use an EMM/MDM server to check and remove certificates from a device over the air.

Certificate pinning

Xperia devices support certificate pinning. Pinned domains will receive a certificate validation failure if the certificate does not chain to a set of expected certificates. This protects against possible compromise of Certificate Authorities.