WHITE PAPER

How to become EPCS Compliant with Gemalto SafeNet Authentication Solutions

Introduction

With one billion digital prescriptions issued annually in the US, and 130 million of those prescriptions accounting for controlled substances, the DEA's Electronic Prescriptions for Controlled Substances (EPCS) regulation provides patients with better care and increased convenience.

Reducing prescription errors, preventing prescription fraud, and allowing the integration of e-prescriptions into electronic healthcare records (EHRs) for the overall improvement of patient care, including their transmission to pharmacies for fulfillment and in-person pickup, EPCS is a hallmark of the HITECH Act, which aims to brings America's healthcare into the information age.

EPCS sets out requirements for issuing prescriptions for controlled substances in digital form, with adoption among healthcare providers growing rapidly in recent years thanks to federal financial incentive programs, as well as state-wide EPCS mandates.

Complying with EPCS

Anyone issuing, transmitting, receiving, and fulfilling an e-prescription (eRx) for controlled substances has to comply with EPCS requirements. Hospitals, medical practitioners (physicians, dentists, nurses), pharmacies, and health information networks all have to comply with the regulation.

In order to gain compliance with EPCS and enable the issuing of e-prescriptions for controlled substances, hospitals and healthcare institutions must instate EPCS-certified processes relevant to:

- Identity-proofing their medical practitioners
- Setting logical access controls to eRx applications
- Using a two-factor authentication (2FA) method to sign each eRx
- Using eRx applications periodically audited by a third party

Best practices for choosing two-factor authentication for EPCS compliance

Consider solutions that offer:

- FIPS 140-2 certification
- Quick and easy deployment
- Low operational overhead
- Flexibility and scalability
- Low TCO

Advantages of deploying Gemalto SafeNet Authentication Solutions for EPCS compliance:

- Fully compliant with EPCS
- Proven security
- Frictionless authentication for practitioners
- Frictionless management for IT administrators

These processes must be audited by a third party, such as a certifying organization **approved by the DEA**[1] or other third-party auditor who can certify that their processes are EPCS-compliant.

EPCS Compliance Schedules

EPCS compliance deadlines vary from state to state, with some mandating compliance as soon as March 2015 (New York, for example) and other states allowing compliance at later dates.

Hospitals and CAHs taking part in a Medicare or Medicaid EHR Incentive Program can demonstrate Stage 2 'Meaningful Use ' by issuing e-prescriptions, including e-prescriptions for controlled substances (EPCS). Specifically, over 10% of all prescriptions issued by a hospital must be issued in digital form for hospitals to meet e-prescription Meaningful Use objectives.

For these organizations, Stage 2 spans the entire duration of the fiscal year following the successful completion of Stage 1 requirements.

[1] http://www.deadiversion.usdoj.gov/ecomm/e_rx/thirdparty.htm

EPCS Authentication Requirements

Under the **Interim Final Rule**[2] of March 2010, the DEA is allowing the use of two of the following methods for eRX signing:

- Something you know – a password or PIN
- Something you have – a hard token stored separately from the computer being accessed
- Something you are – biometric information, such as a fingerprint

Hardware Tokens

When using the combination of a password or PIN with a hardware token, the DEA requires that the token be "stored on a device that is separate from the computer being used to access the application." Examples of hardware tokens include:

- Smartphone
- Tablet
- Smart card
- USB token

In addition, the cryptographic module of the token must be FIPS 140–2 Security Level 1 certified [3].

Software Tokens

Software tokens can also be used, as long as they are installed on a separate hardware device such as those listed above. As with hardware tokens, software tokens must be FIPS 140-2 Security Level 1 certified, meaning that their cryptographic modules are FIPS approved.

Two-factor authentication methods that are prohibited for use under EPCS include out-of-band authentication (OOBA) and any device that is not FIPS 140-2 Security Level 1 certified.

1 Frictionless Management for IT Administrators

- Fully automated lifecycle administration of users and tokens
- Automated solution management via email or SMS text message alerts
- User self-service portals
- Broad integration capabilities
- Cloud and on-premises delivery

2 Frictionless Authentication for Users

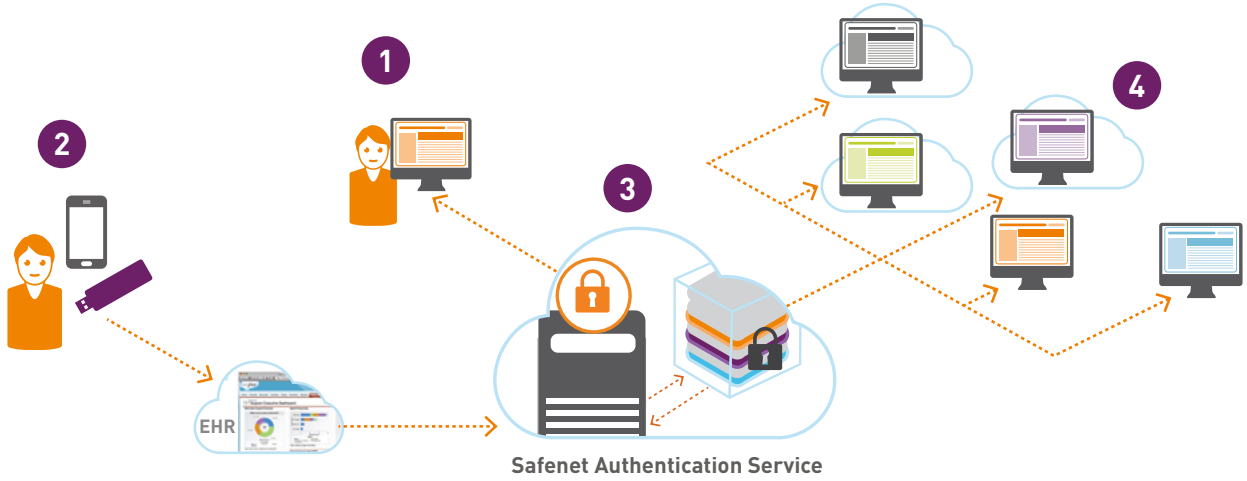
- Free EPCS-compliant software tokens (OTP apps) for a range of mobile devices
- Choice of EPCS-compliant smart cards and USB tokens
- Federated login to the cloud

3 Single Point of Management

Apply consistent access controls to your entire IT ecosystem

4 Complete Use Case Coverage

- 100 seamless out-of-the-box integrations
- VDI
- VPN
- Web Portals
- LAN
- Cloud



[2] http://www.gpo.gov/fdsys/pkg/FR-2010-03-31/pdf/2010-6687.pdf

[3] FIPS 140-2 Security Level 1 refers to the software component of a cryptographic device, namely the cryptographic module. As such, FIPS certification does not refer to hardware or software tokens in their entirety; rather it refers only to their cryptographic modules.

Best Practices for Choosing an Advanced Authentication Solution

When considering a 2FA solution for implementing EPCS within your organization, evaluate solution candidates for the criteria detailed below.

Verify that the solution is FIPS 140-2 approved

In order to be EPCS compliant, 2FA solutions used to sign e-prescriptions for controlled substances must be FIPS 140-2 Security Level 1 approved. Tokens whose crypto modules are FIPS 140-2 certified enable compliance with this requirement, whether they are based on PKI (x.509) certificates or OTPs.

Additionally, an authentication solution that offers a range of authentication methods and form factors, such as certificate-based smart cards and OTP device-as-a-token methods, allows addressing different levels of assurance and offers practitioners a choice, depending on their user preferences and security needs. Compatibility with current infrastructure should also be considered in order to reduce implementation costs and keep time-to-compliance short. For example, are USB ports available on all systems from which controlled-substance e-prescriptions are issued?

Consider a solution that offers quick and easy deployment

To demonstrate EPCS-compliance within the appropriate timeframes (your state's deadline, or the entire fiscal year after the successful completion of Stage 1 requirements), seek a solution that offers quick and easy setup. Features that simplify deployment include:

- **Authentication-as-a-service** delivered from the cloud, which removes hardware and software compatibility issues and supports your current infrastructure with only a short setup process.
- **Software-based authentication methods**, which allow over-the-air provisioning together with automated policy enforcement, as well as other automated lifecycle administration benefits.
- **MobilePKI** allows for the extension of PKI security to mobile devices. By using Bluetooth Low Energy enabled badge holders and tokens, the same credential can be used with devices lacking a card reader or USB slot.

Seek a solution that offers low day-to-day management overhead

To keep ongoing operational costs low, opt for solutions that require minimal intervention by IT staff, through such features as:

- **Automated user and token lifecycle administration**, providing auto-provisioning, auto-modification, and auto-revocation of permissions, accounts, and tokens to practitioners.
- **Automated solution management** via red flag alerts, ideally delivered directly to administrators via email or SMS text messages, containing configurable event- and threshold-based notifications.

Management Platforms

- SafeNet Authentication Service
- SafeNet Authentication Manager

EPCS-compliant Form Factors

- Software tokens (OTP apps) supporting all leading mobile platforms
- Smart cards
- USB tokens

- **Comprehensive self-service portals** that lighten help desk workloads by allowing practitioners to report or resolve numerous issues by themselves; for example, resetting their password or PIN, updating their profile details, reporting a token lost, and so on.
- **Automated reporting,** ideally with reports that are both template-based and customizable, and can be automatically delivered to the appropriate recipients.

Look for a solution that adapts and scales with your ecosystem

Market dynamics, such as mergers and acquisitions, and an ever-evolving IT ecosystem that increasingly spans virtualized and cloud-based resources, makes it important to seek a solution that can accommodate your current infrastructure while letting you adopt new technologies with ease. To this end, select a solution that offers:

- **A broad range of integration methods** – While APIs enable customized homegrown development, SAML-based authentication, as well as application-specific agents and RADIUS-based authentication enable out-of-the-box compatibility with a wide range of healthcare and enterprise IT resources.
- **Multi-tier, multi-tenant architecture** – Support complex organizational structures by leveraging multi-tier, multi-tenant architecture, which lets you quickly on-board new healthcare functions and departments, while separately managing the billing, security, and reporting of each.

Consider a solution that allows meeting budget expectations

By selecting a solution that meets all the above considerations, you will have effortlessly chosen an EPCS-compliant solution that also helps you meet budget expectations. Out-of-the-box integrations, low day-to-day management overhead, support for multiple FIPS-certified 2FA methods, and a simple and quick deployment all make it easier to comply with EPCS while keeping within your budget.

Gemalto SafeNet Authentication Solutions for EPCS Compliance

SafeNet Authentication Solutions by Gemalto enable hospitals and Critical Access Hospitals (CAHs) to meet the DEA's EPCS requirements for two-factor authentication with a fully automated strong authentication solution that can be delivered as a cloud-based service or installed on-premises at an organization's data center.

To achieve EPCS compliance, choose the solution most suitable for your organization:

- Gemalto SafeNet Authentication Service with SafeNet MobilePASS one-time password (OTP) tokens
- Gemalto SafeNet Authentication Manager with certificate-based authentication (CBA) tokens and smart cards

SafeNet Authentication Service with SafeNet MobilePASS software tokens

Providing fully automated over-the-air administration and deployment, Gemalto's SafeNet MobilePASS software tokens meet the DEA's requirement for FIPS 140-2 and can be managed from the SafeNet Authentication Service management platform, delivered on-premises or from the cloud.

SafeNet Authentication Service

Offering multi-tier, multi-tenant architecture, SafeNet Authentication Service delivers fully-automated, highly secure authentication-as-a-service that accommodates complex organizational structures. SafeNet Authentication Service offers fully brandable interfaces and supports both generic and customized workflows, addressing the billing and accounting needs of subsidiaries and affiliate bodies.

To reduce IT administration overhead, SafeNet Authentication Service provides fully automated workflows, including automated lifecycle administration of users and tokens, configurable alerts delivered directly to IT staff via email or text messages, and self-service portals that lighten help desk workloads.

In addition to integrating with prescription-signing applications, SafeNet Authentication Service can be extended to provide a future-ready strong authentication framework for securing a range of resources, including local networks, remote networks (VPNs), web portals, virtual infrastructures (VDI), and cloud-based applications (SaaS).

Increasing transparency and compliance, SafeNet Authentication Service offers a single point of management that produces a single audit trail of all access events throughout the IT ecosystem, as well as automated and granular reporting options, including ready-to-go templates for a range of compliance needs.

SafeNet MobilePASS

Gemalto's SafeNet MobilePASS family of one-time password (OTP) apps combines the security of proven two-factor strong authentication (2FA) with the convenience of OTPs generated on personal mobile devices. SafeNet MobilePASS software tokens feature industry-recognized security standards, including FIPS 140-2 Security Level 1-approved crypto libraries, secure DSKPP provisioning that protects seed confidentiality during over-the-air provisioning, and dynamic reseeding that ensures organizations control their own token seed data by allowing them to reprogram tokens on demand, on-the-fly.

Available for all leading mobile platforms, SafeNet MobilePASS tokens eliminate the need to carry an additional security prop, and remove reliance on smart card readers and the availability of USB ports.

SafeNet Authentication Manager with CBA hardware tokens and smart cards

SafeNet Authentication Manager is a comprehensive authentication server that provides a single point of management for diverse authentication methods, and enables implementation of an adaptable strong authentication strategy.

SafeNet Authentication Manager features complete lifecycle administration, including PKI certificate lifecycle management, token assignment, enrollment and update, self-service portals, and temporary token provisioning. It supports a broad range of strong authentication methods, including PKI certificate-based authentication (CBA), OTP, out-of-band authentication, and context-based authentication with customizable step-up authentication policies.

In addition to integrating with prescription-signing applications, SafeNet Authentication Manager can be leveraged to enforce access control policies on a wide range of resources, including VPNs, cloud (SaaS), VDI, web portals, and local networks.

Certificate-based Hardware Tokens and Smart Cards

Gemalto offers a choice of FIPS 140-2-certified certificate-based tokens and smart cards. Smart cards offer the added value of doubling as photo identification and can also be equipped with physical access controls. USB tokens offer the added value of doubling as secure thumb drives.

Both form factors can be branded with an organization's design scheme and logo.

In addition to supporting digital signatures on e-prescriptions, SafeNet's CBA tokens and smart cards also support multiple advanced use cases, such as email encryption, full disk encryption, pre-boot authentication, smart card network logon and strong two-factor authentication. With MobilePKI, organizations can extend their PKI solutions to mobile devices.

A Fully Trusted Authentication Environment

Providing peace of mind, Gemalto's solutions provide a fully trusted authentication environment based on industry-recognized algorithms and protocols. Our solutions have been certified by regional and international security standards bodies, including FIPS and AICPA in the US, Common Criteria in the EU, and the International Standards Organization (ISO). Gemalto's tokens are field-programmable, allowing customers to retain stringent control over their own token seed data, and our solutions are secured with a hardware-based root of trust.

About Gemalto's SafeNet Identity and Data Protection Solutions

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core.

Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters.

Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com
Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free