Allscripts EPCS Credential Service Provider (CSP) changing to ID.me

Frequently Asked Questions

CSP Change and Customer Impact

Q: What is a CSP?

A: A CSP (Credential Service Provider) is a trusted entity that issues security tokens (electronic credentials) to users of software. A CSP forms part of a complete authentication system and is typically separate from the application software itself. CSPs can, and often do, perform identity proofing as part of securely issuing credentials to a user.

Q: What is the purpose of identity proofing and how does it work?

A: Identity proofing is designed to securely establish a digital identity for an individual. The process itself provides the following assurances:

- A person with the presented information exists in society.
- The person presenting the information to the system is, in fact, that individual.
- No other person could likely pretend to be the identity being presented.

The above approach, established by NIST, aims to ensure that users of applications and systems are who they claim to be.

Q: How are CSPs related to EPCS?

A: Under DEA regulations, all EPCS software vendors must integrate with a federally approved CSP to enable providers to issue controlled substance prescriptions electronically. Allscripts, as an EPCS software vendor, must adhere to these regulations and provide such capabilities.

Q: Why is Allscripts changing its CSP?

A: Allscripts is changing its CSP vendor to ID.me because its current CSP, Zentry (formerly known as Verizon), has informed Allscripts that it intends to exit the CSP business in 2019.

Q: Which clients will be affected by this change? What EHR versions are affected?

A: Allscripts clients using Sunrise™, Allscripts TouchWorks®, Allscripts Professional EHR™, or Allscripts ePrescribe for Electronic Prescribing of Controlled Substances (EPCS), who use Zentry as their CSP. Clients using Imprivata ConfirmID are not affected by this change.

Q: Will customers need to upgrade their EHR software to support ID.me?

A: No EHR upgrade is required during this initial stage. For Professional EHR customers with versions 17.1 and earlier, a server patch will be delivered by Professional Services.
For those using Veradigm ePrescribe, ID.me will be available early April in ePrescribe 2019.1.0

Q: Will the EHR products need to be re-certified to use ID.me?

A: No re-certification of the various Allscripts EHR products is required. The change is happening in the Allscripts EPCS cloud solution. The Allscripts EPCS cloud solution will be re-certified under DEA regulations.

Q: What do customers/prescribers need to do?

A: All EPCS Prescribers will need enroll with ID.me and link the new ID.me account to their existing Allscripts Security Account.

Q: When will the new enrollment Site with ID.me be available? When can prescribers start to enroll and transition to ID.me?

A: A new CSP enrollment and management website will be made available in March 2019 to facilitate user enrollment with ID.me. Once the new website is online, prescribers will be able to create a new ID.me account and link it to their existing Allscripts Security Account (ASA).

Q: What options are available to new customers and providers?

A: After the CSP management website is available, new prescribers will follow the same process as currently established in their EHR software, with the difference that the prescriber will need to create an ID.me CSP account of instead of a Zentry account.

Q: Why do prescribers have to re-enroll? Why can't our account be transferred over to ID.me?

A: The CSP vendors have no capacity to security transfer accounts between one another. Zentry is exiting the CSP business and for both technical and security reasons, ID.me cannot accept existing identities established under Zentry.

EPCS Proofing Models

Q: What is the difference between the EPCS Institutional or Individual models?

A: The DEA defines two (2) models for credential use in the EPCS program:

- Individual Practitioner (e.g., a physician, dentist, veterinarian, or nurse practitioner that is a DEA registrant lawfully permitted to prescribe controlled substances)
- Institutional Practitioner (e.g., a hospital or clinic that is a DEA registrant lawfully permitted to prescribe controlled substances).

Clinicians can prescribe controlled substance prescriptions under either model. The *Institutional* model was defined to be an in-person proofing model, while the Individual model was defined to be a remote proofing process.

Refer to the DEA's Interim Final Rule with Request for Comment - Questions and Answers for Prescribing Practitioners for more details.

The DEA regulations state that authentication credentials used to sign controlled substance prescriptions are issued only to the individuals whose identity has been confirmed.

Extract from DEA EPCS FAQ:

https://www.deadiversion.usdoj.gov/ecomm/e_rx/faq/practitioners.htm#individual

"….**Individual practitioners** will be required to apply to certain Federally approved credential service providers (CSPs) or certification authorities (CAs) to obtain their two-factor authentication credential or digital certificate. The CSP or CA will be **required to conduct identity proofing** that meets National Institute of Standards and Technology Special Publication 800-63-1 Assurance Level 3. Both in person and remote identity proofing will be acceptable."

https://www.deadiversion.usdoj.gov/ecomm/e_rx/faq/practitioners.htm#institutional

"…DEA is allowing **institutional practitioners**, who are DEA registrants, to conduct the identity proofing for any individual practitioner whom the institutional practitioner is granting access to issue prescriptions using the institution's electronic prescribing application. **Because institutional practitioners have credentialing offices, those offices may conduct in-person identity proofing** as part of the credentialing process. DEA is not requiring institutional practitioners to meet the requirements of National Institute of Standards and Technology Special Publication 800-63-1 for identity proofing. Before the institutional practitioner issues the authentication credential, a person designated by the institutional practitioner must check the individual practitioner's government-issued photographic identification against the person presenting it. The institutional practitioner must also check State licensure and DEA registrations, where applicable."

Here are the current models supported by each product.

Product	Institutional	Individual
Sunrise	**Yes**	No
TouchWorks	**Yes**	**Yes**
ProEHR	No	**Yes**
ePrescribe	**Yes**	**Yes**

Enrollment Process

Q: Why do we have to reset the Allscripts Security Account (ASA) Password? How is this different than the EHR Login?

A: the Allscripts Security Account is created upon initial registration when a user is granted permission to prescribe EPCS. After conducting the respective identity verification of the prescriber, the EHR Login is linked to the Allscripts Security Account.
Since the ASA is rarely used directly by EHR users, it is therefore quite probable that users will not recall the original password used when the account was initially enrolled. Within each EHR there is a feature to reset the ASA password that does not require to know the previous password. To ensure a smooth enrollment, we are requesting users to reset their ASA password as the first step of the enrollment process.

Q: Will Prescribers have to get Re-identity proofed online with ID.me?

A: Only individual prescribers will be required to establish their identity with ID.me. ID.me uses newer approaches to identity proofing individuals while Zentry's technology was based on legacy standards for user identity proofing. Zentry relied on knowledge-based assessments (KBA) and financial inquiries to determine the existence and ownership of a claimed identity. ID.me, however, uses a combination of identity evidence factors, 3rd party data integrations, Financial and Utility verifications to identity proof a user without prompting the user with KBAs The ID.me proofing software uses modern reader technology that can read the information from a Driver's License or a Passport using a smartphone. For those cases that their identity cannot be established online, the prescriber can schedule a video conference with an authorized ID.me Referee to conduct a remote-proofing session to verify the supplied information and establish the identity of the prescriber. No more Manual Notary public forms. Online Identity Proofing is only required for Individual prescribers. Institutional prescribers' identity is verified by the Hospital or clinic credential office.

How does the ID.me identity proofing process differ from the existing Zentry identity proofing process?

A: ID.me uses the latest NIST 800-63-3 Identity Proofing methods that allow the use of modern reader technology that can read the information from a Driver's License or a Passport and compare against a selfie image. ID.me uses a combination of identity evidence factors, 3rd party data integrations, Financial and Utility verifications to identity proof a user without prompting the user with KBAs. Zentry relied on knowledge-based assessments (KBA) and financial inquiries to determine the existence and ownership of a claimed identity. With ID.me, for those cases that their identity cannot be established online, the prescriber will be prompted to schedule a Virtual in-person video conference to complete identity proofing with a Trusted Referee. No more Manual Notary public forms.

Q: When does the Video conference come into play?

A: While traditional online identity proofing helps most users access secure services online some of the common reasons that prevent a person's identity to be verified online are: Credit Freeze or limited credit files, outdated information stored in credit bureaus, lack of permanent

address and unregistered prepaid phones among others. For those cases a Virtual in-person proofing allows those individuals to complete identity proofing with a trained Trusted Referee via a simple video conference session. During enrollment users will be prompted to schedule a video conference with a Trusted Referee after they fail online identity proofing. Information previously entered during the online proofing process is pre-populated during virtual in-person proofing, saving users the hassle of re-entering their information more than once. Less than 10% of proofing cases are expected to be completed by a Virtual In-Person session.

Q: What is a Trusted Referee? How do we know if our organization will need a Trusted Referee?

A: A Trusted Referee is a person that has been Identity proofed at the highest level, IAL3, has taken a course, and passed an exam. A Trusted Referee is part of the ID.me Credentialing services and only comes into play when the identity of an individual practitioner cannot be verified online. Less than 10% of individual practitioners are expected to not be able to complete verification online and would require a Trusted Referee. This only applies for Individual model. Institutional customers are responsible to identity proof of the prescribers using their EHR and therefore are not required to be identity proofed by the CSP (ID.me) . Additionally, ID.me has Trusted Referees available to handle the expected load and more Trusted Referees can be added should the need arise. For EPCS enrollments, there is no need for your organization to have a Trusted Referee staff, this is part of our EPCS Service.

Q: What if a prescriber has a credit Freeze on the account?

A: They should receive a notification from their Credit Freeze Service of the credit inquiry and your online identity proofing will most likely fail. In the such case, a Virtual In-person session with a ID.me Trusted Referee will allow to complete the proofing process.

Q: Can we create an ID.me account now before enrollment website is online?

A: While it is possible to create a basic ID.me account before GA, we encourage users to wait because the prescriber will still need to login into the Allscripts CSP Management Site to link their ID.me account to the Allscripts Security Account. Additionally, depending on the customer model, the user may need to complete online proofing before ID.me authenticators can be used for EPCS. The time gained is minimal at best and users have more than 3 months to complete a 2 to 5-minute enrollment.

2FA Options

Q: Will prescribers be able use their existing Zentry/Verizon credentials (Soft Token, Hard Token/Key Fob) after they enroll with ID.me?

A: Yes, but only until the Zentry service is no longer available.

Q: After signing up with ID.me, how will prescribers configure their 2FA options?

A: After registering with ID.me, prescribers will be able to configure their 2FA options by launching from EHR to the CSP Management Site or going directly to ID.me and clicking on "Account Security"

Q: What is replacing Hard Token key fobs? And what is to be done with the existing fobs?

A: The existing One Time Password (OTP) Hard token Key fob can be continued to be used up to when Zentry terminates service, at which point the OTP Hard token will become obsolete and

can no longer be used or re-used. Prescribers can throw away or keep as souvenir. The equivalent functional replacement for the Key Fobs is a newer generation of authenticators called FIDO U2F (Fast Identity Online Universal second factor). Support for FIDO will be made available a later phase and will require an EHR upgrade.

Q: What is a Soft token App and how is it used? Is this the same as the ID.me Authenticator App?

A: A soft token app is an application that generates a 6 digit Time bound One Time Password (OTP) code very similar to code generated by the Hard Token OTP Key Fob. ID.me's soft token app is called the ID.me Authenticator app and it will run on iOS 10.3 and above or an Android (including tablets) Version 6 (Marsh mellow) .

Q: What about prescribers that do not have a smartphone or do not want to use their personal phones?

A: If the use of a personal phone is not viable and/or a prescriber does not have a smartphone, a tablet (iOS or Android) can be used with the ID.me Soft Token App as the second authenticator device.

Q: Why is SMS and IVR being removed as a 2fa option? What is replacing SMS?

A: SMS and IVR have been placed on the RESTRICTED Authenticators list as these have been proven to be insecure. We have been instructed by our DEA Auditors to phase out the use of SMS and/IVR as 2FA option for the EPCS. A more secure form of authentication than SMS is the ID.me Authenticator App that meets FIPS 140-2 Level 1 Compliance as required by DEA/NIST. Another form of notification like SMS but much more secure is PUSH NOTIFICATIONS which provides a faster and easier way to authenticate.

Q: What is FIDO and how will it be used? Are these the new key fobs?

A: The FIDO Alliance ("Fast IDentity Online") is an industry consortium launched in February 2013 to address the lack of interoperability among strong authentication devices and the problems users face creating and remembering multiple usernames and passwords. *See https://fidoalliance.org/ and https://en.wikipedia.org/wiki/FIDO_Alliance.*

FIDO-compliant devices are cryptographic devices that comply with the FIDO standards defined by the FIDO Alliance. Yubico is a manufacturer and vendor of FIDO-compliant hardware authentication devices. Yubikey is the brand name for the devices they manufacture. More details and examples can be found here: https://www.yubico.com/.

FIDO devices come in either a USB or NFC and when prompted to use by the software, the simple presence of the FIDO device will be sufficient as the "something you have" second universal factor.

Q: What is a Push Notification and how will it be used?

A: Push notifications are easier and a more secure form of authentication using the ID.me Authenticator app. Upon signing a prescription, the prescriber will receive a notification on their smartphone for an authentication request. The approval is authenticated with a Biometric scan (finger print or face) or a user chosen Pin code, and upon successful match, the prescription will be signed and submitted. There is no need to read and type in a 6 digit OTP code.

Miscellaneous

Q: What is going to happen with prescribers that prescribe at different locations? How will they handle administrating more than one account? (Multi-Tenant Scenario)

A: Prescriber's that practice at more than one Location/Site (tenant), will currently have per location/tenant, an Allscripts Security Account (tenant) and a Zentry CSP account. We will provide detailed instructions on how to transition to ID.me before we go live. We are aware of the situation/shortcoming and are working with our auditors to explore compliant options address this scenario.

Q: Once a user enrolls in Id.me, can they "switch back" to Zentry?

A: Users don't "switch" between different CSP vendors. Users can have accounts with both Zentry and ID.me simultaneously. Additionally, so long as the user has achieved the requisite identity proofing level with the CSP account, they can use that account during EPCS workflows.

Q: For the Institutional model, if a provider has already been credentialed by the hospital, will they have to be re-credentialed by the Hospital in order to switch to ID.me?

A: No. The user will simply enroll in ID.me and begin using the ID.me credential as their 2nd-factor authentication credential during EPCS workflows.

Q: How will users without a smartphone complete the ID.me enrollment process?

A: The ID.me enrollment workflow can be completed via a web browser on any device. The enrollment process does require the user to be able to receive a text message on a mobile phone. However, the workflow does support "non-smartphone" devices and the user will be presented with a screen to select the option that works best for them.

Q: Will a User Acceptance Test (UAT) environment be made available?

A: Yes, the Allscripts EPCS Cloud service UAT environment will be linked to the ID.me Production environment