Using Two-Factor Authentication

A white paper by:
Andreas Dieckow
Principal Product Manager
InterSystems Corporation

InterSystems®

Using Two-Factor Authentication

Introduction

If the administrators responsible for securing applications had their way, passwords would be long complex strings of random symbols, and users would memorize different passwords for every application they use. But in the real world, few people are capable of such prodigious feats of memory. The typical user can only remember a handful of relatively short passwords.

That's why an increasing number of applications are requiring two-factor authentication. In addition to asking for a password (something the user knows), applications can be configured to ask for a supplementary password delivered in real time via a device (something the user has). Two-factor authentication provides an extra layer of assurance that the person logging on to an application is, in fact, who he or she claims to be.

This paper outlines how InterSystems supports two-factor authentication in all of our products.

What is Two-Factor Authentication?

With two-factor authentication, users are granted access to an application based on a) something they know, and b) something they have. The most familiar implementation of two-factor authentication is probably a bank's ATM system. The "something users have" is an ATM card. The "something users know" is a PIN. However, ATM systems are limited because they require use of a physical ATM machine that can read a user's card.

Another example of two-factor authentication is use of a dedicated device (for example, an RSA device). When logging on to a protected application, users will be prompted both for their password (something they know) and a token provided by their dedicated device (something they have). Dedicated devices generate tokens by using a cryptographic hash function to combine a secret key with the current time. The secret key is shared between the dedicated device and the server that is granting access to the application, so the server will be able to verify the token.

Hardware vs. Software for Two-Factor Authentication

Dedicated devices are an example of hardware-based two-factor authentication. The "something people have" (a dedicated device) is a physical object that exists solely for the purpose of providing an extra element of security.

This paper deals with software-based two-factor authentication. The "something users have" will be some sort of smart device capable – among many other functions – of running software. When users log on to the application they wish to access, they will receive a token, via their smart device, that must be entered before access is granted.

There is a growing trend towards using software-based, rather than hardware-based, two-factor authentication. One reason is simply convenience. Many people own phones or other smart devices capable of running an app that can generate tokens. That being the case, there is no need to also carry a "dumb" device that exists only to help the two-factor authentication process.

There's a physical security benefit too. People tend to be dependent on their phone, and they very quickly notice if it goes missing. However, people probably won't realize they've misplaced a dedicated device until they actually need to use it. The window of opportunity for a malicious attack is much smaller in the case of using software-based two-factor authentication.

Another benefit of using software-based two-factor authentication is that a smart device can hold multiple shared secret keys. Different applications can be configured with different secret keys. In the event that one secret key is compromised, only one protected application will be in jeopardy.

InterSystems Support for Two-Factor Authentication

InterSystems supports two approaches to implementing software-based two-factor authentication: Short Message Service (SMS)-based, and Time-based One-time Password (TOTP). An end-user can be configured to use both mechanisms, but only one can be enabled at a time.

SMS-based

When using SMS-based two-factor authentication, a text message containing the token is sent to a user's smart device. The benefit of this approach is that it is relatively easy to provision users – part of the requirements for being added to the system is that users provide a phone number or email address where text messages can be sent.

The drawback to SMS-based two-factor authentication is that it requires users to have a cell phone signal in order for the authentication process to function. In places where there is no cell signal, or where cell phone use is not allowed or is blocked, users will be unable to access the protected application.

Time-based One-time Password (TOTP)

An increasingly popular approach to implementing two-factor authentication is to use a Time-based One-time Password. A TOTP is an example of a hash-based message authentication code (HMAC), and is the software-based equivalent of using a dedicated device. With the TOTP approach, a unique secret key is shared between the application server and an app running on a user's smart device. When the user logs on, the app uses that key and the time to generate a token. Because the secret key is shared by both the application server and the user's smart device, the same token will be generated.

The advantage to using a TOTP is that users don't need a cell phone signal in order to authenticate themselves to the application. The disadvantage is that the secret key must be downloaded to an app running on the user's phone, which can make provisioning a challenge.

Provisioning TOTP

InterSystems' support for TOTP implements the RFC 6238 standard to generate time-based, one-time passwords. The first requirement for using the TOTP approach to two-factor authentication is that the user must have an authentication device or an app that implements the same standard. For example, a user might use one the following apps for mobile phones:

- Google Authenticator, for Android, Blackberry, or iPhone
- DuoMobile, for Android or iPhone
- Amazon AWS MFA, for Android
- Authenticator, for Windows Phone 7

Once the authentication software has been downloaded, a user must input three pieces of information:

- Issuer: the name of the application that is issuing the key. (For applications based on InterSystems' products, this will be an instance of Caché.)
- Account: the user's account name
- Shared key: a base-32 encoded random bit string generated by Caché

The most secure way of sharing this information is to provide it to the user either in person or by phone and have the user enter it manually. However, that process can be cumbersome and error prone, especially if many users will need to be authenticated to the application.

For convenience, Caché generates a QR code that the user can scan in order to enter the information. Using a QR code makes provisioning easier, but care must be taken that the QR code is not transmitted by the same channel that is to be secured.

Conclusion

Two-factor authentication can provide extra assurance that users are who they claim to be. InterSystems supports both SMS-based and TOTP two-factor authentication for all our products.

InterSystems Corporation

World Headquarters
One Memorial Drive
Cambridge, MA 02142-1356
Tel: +1.617.621.0600

InterSystems.com