Secure Robotic Process Automation for Government Agencies

HIGHLIGHTS

- Enable software robots to perform tedious tasks without creating security vulnerabilities
- Use high assurance PKI to enhance the security of robotic process automation
- Secure critical private cryptographic keys in FIPS-certified hardware security modules (HSMs)
- Helps meet OMB Memo M-19-17 requirements for the management of digital identities

THE CHALLENGE

Authenticating RPAs with more than just a password

As U.S. federal government agencies strive to operate more efficiently, robotic process automation (RPA) is increasingly being used. RPA robots capture and interpret data, trigger responses, and communicate with other systems in order to perform repetitive tasks without the risk of human error.

Deploying these systems securely requires high assurance authentication mechanisms, which is not as straightforward as authenticating human users. Government agencies require multifactor authentication (MFA) for employees to access most computer networks. For these users, this means having both a personal identity verification credential (PIV card) and entering a personal identification number (PIN).

But when RPA robots act as system users, they don’t have PIV cards for authentication. Traditionally, robots logging into agency systems used only passwords, making them a weak link in the overall security system. All a cybercriminal or nation-state actor needed in order to access sensitive systems was to guess the password.

So how do you fully secure digital robots performing functions previously done by humans?

The Office of Management and Budget Memo M-19-17 sets forth a policy for Identity, Credential, and Access Management (ICAM), including for any **“non-person entity (NPE), or an automated technology, that is engaged in a transaction involving at least one Federal subject or a Federal resource, for example, Federal information, a Federal information system ...”**

According to this policy, devices and NPEs must have digital identities that are **“distinguishable, auditable, and consistently managed”** and that can be updated or revoked as needed.

Secure Robotic Process Automation for Government Agencies

THE SOLUTION

UiPath RPAs + Entrust nShield HSMs

Because the robots cannot hold PIV credentials, Entrust and UiPath have collaborated on a robust solution to facilitate high assurance certificate-based authentication for UiPath robots using your existing public key infrastructure (PKI).

UiPath software robots are flexible, reliable, and can handle repetitive tasks across desktop, web, Citrix, and other interfaces, as well as enterprise applications from SAP, Oracle, Microsoft, and many others. These robots can automate a wide range of tedious processes, allowing skilled employees to focus on higher-value activities.

The certificates issued to each robot are underpinned by private keys that are protected by Entrust nShield® Connect Hardware Security Modules (HSMs).

The combination of UiPath RPA and Entrust nShield HSMs allows government agencies to deploy software robots that meet strict federal security standards.

FEATURES AND BENEFITS

Entrust nShield Connect HSMs are high-performance network-attached devices that:

- Provide a FIPS 140-2 and Common Criteria certified root of trust for the private keys that underpin UiPath RPA robot credentials
- Provide a proven and auditable way to secure valuable cryptographic material
- Ensure the RPAs are never slowed down when calling on the HSM for authentication
- Protect keys that underpin digital certificates within a certified, hardened cryptographic boundary, safeguarding them from attacks that can lead to compromise of confidential information
- Ensure availability by using sophisticated key management, storage, and redundancy features to ensure keys are always accessible when needed, and only used for their authorized purpose

UiPath™ ENTRUST

Secure Robotic Process Automation for Government Agencies

ABOUT US

UiPath

UiPath has a vision to deliver **a robot for every person** so companies can enable every employee to use, create, and benefit from the transformative power of automation to liberate the boundless potential of people.

UiPath offers an end-to-end platform for automation, combining the leading RPA solution with a full suite of capabilities that enable every organization to scale digital business operations at unprecedented speed.

Entrust nShield HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easiest-to-integrate HSMs available. They help facilitate regulatory compliance and deliver the highest levels of data and application security for enterprise, financial, and government organizations.

Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

LEARN MORE

To learn more about UiPath, go to uipath.com.

To learn more about Entrust nShield HSMs, go to entrust.com/HSM.

To learn more about Entrust digital security solutions for identities, access, communications, and data, go to entrust.com.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact