Robotic Process Automation (RPA) Within Federal Identity Management

After spending almost 15 years implementing Homeland Security Presidential Directive 12 (HSPD-12) solutions to identify and provision human users in Federal information systems, how do we design secure identity solutions for the emerging Digital Workforce?

Introduction
RPA uses software robots—also known as bots—which are software applications designed to automate transactional, rule-based tasks by mimicking user interactions. RPA can reduce risks and save workers time by automating time-consuming, tedious, and error-prone tasks, such as performing monthly account reconciliation activities based on established rules and manual processes. RPA solutions have existed for over a decade, but with recent advancements in technology, they have seen wider deployment in businesses today and have been encouraged by the Office of Management and Budget (OMB) as a potential solution to redirect limited resources to accomplish mission outcomes that matter most to citizens (Memorandum M-18-23 Shifting From Low-Value to High-Value Work). Given the on-going adoption of RPA, securing bots and paying close attention to how they are access systems and data is critical. Existing identity management tools and related security control configurations, such as the adoption of HSPD-12/Personal Identity Verification (PIV) credentials, the implementation of mutual Transport Layer Security (TLS) authentication or other multi-factor authentication mechanisms, have proven effective in securing Federal IT systems. Using these technologies, organizations can facilitate secure, auditable access for human and digital users alike.
While many out-of-the-box RPA solutions may have organic credential managers allowing bots to login to applications, these credentials generally include a standard ‘knowledge-based’ replay feature that leverage user names and passwords. These credentials may not be strong enough to access Federal applications or information that require higher authentication assurance and contain sensitive data. To accomplish this, Public Key Infrastructure (PKI)-based credentials can be issued to bots in accordance with established Federal certificate issuance capabilities.

**Common Use Cases**

Both industry and government organizations are realizing the potential for increased productivity gained through the adoption of RPA. Common use cases of RPA can include, but are not limited to:

- Automated reports generation and communication
- Email alert management
- Financial account reconciliation
- Payroll automation
- Inventory record keeping
- Virtual assistants or ‘chat bots’
- Data lifecycle management
- Vulnerability analysis

This push to automate process execution drives the need to properly identify, provision, and manage bots in an architecture centered around trusted personal identification.

**Traditional Identity Management in the Federal Government**

Traditional identity management within the Federal Government has been highly focused on vetting and credentialing humans (e.g., issuing PIV credentials to the workforce), as well as establishing trusted identities for verified applications and servers (known as devices or Non-Person Entities [NPEs]). Prior to the recent development of RPA tools, there was little business need to develop specific standards, policy, or implementation guidance specifically for creating or managing digital worker identities. Given the contemporary interest in the digital workforce and its associated ability to act in a manner similar to human users, it is likely that existing identity management solutions can support the identification and accesses required for the emerging digital workforce.

**Solving Digital Workforce Identity**

When the use of a higher assurance credential is necessary, due to the National Institute of Standards and Technology (NIST) Federal Information Processing Standards 199 (FIPS 199) system categorization or associated data sensitivity rating, existing PKI mechanisms can enable bot credentialing, authentication and access.

PKI-based solutions such as smartcards or software based certificates and keys, are acceptable for facilitating bot authentication. Most Federal organizations either manage or have acquired PKI services, and are already well positioned to begin issuing and using certificates aimed at identifying bots within their information systems.

Because RPA solutions are not humans, bot certificates should contain information that easily identify Non-Person Entities (NPEs) or devices when they attempt to gain access to applications. As noted in OMB Memorandum M-19-17, titled Enabling Mission Delivery through Improved Identity, Credential, and Access Management, agencies are compelled to ensure the “digital identity is distinguishable, auditable, and consistently managed across the agency”, to include “establishing mechanisms to bind, update, revoke, and destroy credentials for the device or automated technology.” Additionally, human sponsor correlation is required prior to certificate generation to align accountability with potential system misuse. While these two factors are critical in credentialing bots, other significant requirements also deserve careful consideration.

These requirements can be broken into several categories: Policy/Governance, Technical Considerations and Procedural Considerations. Figure 1 below provides high-level examples of each category to be discussed in more depth.
These recommendations leverage established PKI assets and processes in order to optimize existing IT investments and minimize significant process redesign which could impact an organization’s ability to leverage RPA’s productivity benefits while still supporting security requirements.

Critical bot credentialing takeaways include:

1. Human sponsor registration is recommended to assign accountability (legal/privacy/financial), and ensure efficient revocation in the event a sponsor separates from an organization. Implementing this process aligns with the guidance provided in OMB Memorandum M-19-17.
2. Bot certificates should properly reflect identity attributes of NPEs to drive compliance.
3. Bot identities should be uniquely identifiable to increase auditability of their actions.

Finally, the subsequent sections provide additional detail and cover more direct guidance to assist technical implementers and procedural stakeholders to understand the scope of changes that might be required for their systems and workflows.
In-depth Implementation Considerations

Policy/Governance Considerations
While changes may be required to facilitate the registration, issuance and use of bot certificates, other significant high-level decisions are also needed to drive oversight and provide guidance for implementers. Hence, establishing governance during this nascent stage of bot usage by the Federal government will position agencies to comply with security controls as they further deploy bots. For example, it will help to alleviate pilots being developed in a “vacuum,” using implementer’s best guestimates for how to meet yet undeveloped policies. If several agencies begin unique credentialing processes and then are required to update, retool and redeploy these processes due to subsequent guidance becoming available, additional time, resources and expenses would be required for said agencies.

Although some Federal organizations may have established cross-functional governing bodies focused on managing identity, others may only have isolated Program Management Offices (PMOs) focused on limited aspects of identity (e.g., human enrollment or operational PKI services). In an effort to strengthen Identity, Credential and Access Management (ICAM) governance and oversight throughout the Federal government, OMB has recently released a draft memorandum (OMB M-19-17 Enabling Mission Delivery through Improved Identity, Credential, and Access Management) recommending the establishment of such groups within each department to assist in associated decision support, including elements of bot credentialing.

A governing body that oversees identity and access policy may also want to define an acceptable list of use cases or account justifications for bots. Provided the wide variance of risk-based security controls on IT systems, it is feasible that only specific categories of information systems or their associated risk ratings (e.g., FIPS 199 Medium or High) may be appropriate for access with PKI. Additionally, governing bodies may want to define system characteristics or guidelines for use of lower assurance credentials.

Examples of Department-Level Identity Governing Bodies:
• DoD Identity Council
• HHS PKI Policy Authority/HSPD-12 PMO
• DHS HSPD-12 Council
• Treasury PKI PMO

Given RPA is a relatively new use case as it relates to managing identities, especially when leveraging PKI solutions, several documents may require updates to account for new policies or processes. The overarching Certificate Policy (CP) may require updates to account for certificate data fields used to identify subjects (also known as Certificate Policy Object Identifiers). This field value may need to be developed or updated to reflect devices or specifically bots, as well as establish minimum human registration and account justification requirements. Updates to a Registration Practice Statement (RPS) may also be needed to outline the steps employed by a Registration Authority (RA) to support the bot certificate issuance and account application.

PKI form factors used for private key generation and storage will also need in-depth consideration. While it is certainly feasible to leverage smart card form factors for bot private key security (similar to Alternative Tokens), the subsequent activation of the key may create logistical or coordination issues. In these instances, human access to the card and the associated key may require additional auditability as well as physical security controls for the card. Alternatively, bots can also be credentialed with software certificate form factors. In these cases, the private keys can be stored on the local machine that hosts the bots, in the RPA software’s credential vault, or a stand-alone Hardware Security Module (HSM) depending on the agency’s requirements. However, software form factors could create other security concerns, such as key exportability, which is a topic that should be evaluated while Federal governance is being developed.

Additional approval may need to be considered prior to issuance of a bot certificate such as:
• Proof of backend account authorization
• Backend account unique identifiers
• Assertion of sponsor security training
• Signed PKI user agreements or associated ‘Rules of Behavior’
• Information System Security Office (ISSO) bot access approval

If bot credentials are not directly tied to a sponsor’s PIV information (similar to derived credentials), PKI governing bodies will have to consider a maximum validity of bot certificates, or an alternative method to correlate human sponsor PIV/PKI revocation to bot certificate revocation. Prior to standard automated solutions becoming available for this PIV/PKI revocation correlation, there are several expiration options to choose from, such as:
• A standard maximum lifetime such as 12 months
• A correlated expiration based on the requestor’s PIV/Common Access Card (CAC) expiration, or
• A unique bot account expiration date, or planned decommission date

A few corollary governing considerations may also include:

• Coordination of PKI policy and bot use cases with other critical parties, such as system owners

• Potential impacts to Interconnection Security Agreements (ISA) or Memorandum of Understanding (MOU) between applications where bots might be employed

• RPA license management and associated costs for associated PKI credentials

• Risk ratings of relying party systems and minimum security ratings for bot PKI authentication

**Technical Considerations**

Given we have established that PKI is an acceptable solution for credentialing bots, there are still high-level policies developed and maintained by the Federal PKI Policy Authority (FPKIPA) that precipitate technical considerations to assist in driving compliance.

Essentially, an X.509 public certificate is a digital representation of the entity that has control over the associated private key. The certificate itself is just a digital file that contains information about the subject to include the associated public key. As a digital identity, a bot certificate requires certain data fields be properly configured and express detailed information. For those organizations leveraging Federal PKIs, this includes the following identifiers that define the nature of the subject and how the certificate or keys can be used.

<table>
<thead>
<tr>
<th>Certificate field</th>
<th>Acceptable values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Policy OID</td>
<td>id-fpki-common-devices</td>
</tr>
<tr>
<td></td>
<td>id-fpki-common-devices-Hardware</td>
</tr>
<tr>
<td></td>
<td>id-US-dod-mediumNPE</td>
</tr>
<tr>
<td>Key Usage</td>
<td>Digital Signature</td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>Client Authentication</td>
</tr>
<tr>
<td></td>
<td>Smart Card Logon</td>
</tr>
</tbody>
</table>

The **Certificate Policy Object Identifier (CP OID)** is critical to properly expressing certain attributes about the key holder. The CP OIDs listed in the previous table apply to the Federal PKI or DoD PKI, are mapped specifically to devices or non-person entities (NPEs) and are appropriate for bots. These OIDs can also be used to infer what level of cryptographic modules (e.g., smartcard vs. software) the private keys are secured.

Becasue many RPA solutions will be accessing applications or resources through web browsers and authentication portals, both **Key Usage (KU) and Enhanced Key Usage (EUK)** are required to facilitate proper mutual TLS authentication with a hosting server. Without either the digital signature KU or the client authentication EKU, bots may not be prompted by the browser/web-application to authenticate. Organizations examining PKI for identifying their bots should reach out to their associated PKI service providers to coordinate the proper certificate profile development and testing.

Because both the Federal and DoD PKIs are well established with corresponding Certificate Policies, it is recommended they be leveraged to credential bots that will be used through their respective domains or potentially with external parties; however, private or internal PKIs can also be configured to account for bot certificate templates as needed. If private PKIs are used, note that proper CP OID establishment will be required and relying party applications will also need to be able to conduct Path Discovery and Validation (PDVAL), to include revocation checking, on the resulting bot certificates.

Any identity process applied to bots should also validate that bots are **uniquely identified** and distinct from other persons and non-persons in an enterprise. This will facilitate proper account correlation in relying party applications and will assist with audit and logging. Many Federal organizations already employ an approach for uniquely identifying people, such as DoD’s 10 digit Electronic Data Interchange Person Identifier (EDIPi). It is recommended that bot identifiers use a schema that is distinct from person identifiers where possible. However, a bot unique identifier (UID) should be placed in the same data field as a human certificate (e.g., in the Distinguished Name, or as a User Principal Name [UPN] in the Subject Alternate Name) to reduce the configuration changes that might be necessary in applications that already accept PKI for authentication.

Many identity management systems throughout the Federal government are generally configured to store human identities, as a result, bot identities may need to be managed separately, provided governance decisions regarding PKI form factors. This separation of human and device identity may cause issues with traceability and legal liability. Therefore, the bot certificate also carry data **uniquely related to the sponsor**, where feasible. For instance, the human sponsor’s email address or principal name can be expressed in the Subject Alternate Name (SAN) field of the bot certificate.

Finally, it is important to consider whether a system can actually accept bot certificates or not. To this point, organizations are required to determine how accounts will be established for bots in certain applications and what
roles/permissions they will require to complete their tasks. This is particularly important when the target application is not owned by the implementing organization. While the backend account provisioning process is out of scope for this discussion, it is still important to note that the relying party application will need to be capable of storing the bot UID from the certificate in its user directory in order to correlate to an account that will allow the bot to complete its assigned tasks.

Although not directly related to bot credentialing, additional technical security configurations may also need to be taken into consideration to facilitate domain login with the use of bot certificates. For instance the requirement for a bot to enter CTRL+ALT+DEL and accept a user agreement may not be relevant for non-human domain authentication, and may actually cause issues with domain authentication by bots.

**Procedural Considerations**

While there are significant technical considerations that need to be accounted for before a bot certificate is ever issued, there are also multiple procedural planning factors that need to be addressed during registration to validate bot certificates are issued and used in a compliant manner that supports organizational security goals.

The highest priority procedural consideration is the **registration of the human sponsor.** Similar to human registration in support of derived credentials or TLS certificates, human sponsors need to be properly identified and vetted to validate responsibility of the bot is assigned to a known party. As defined in the Federal Information Processing Standard 201-2, there are several processes to identity proof a human, but within the Federal space, the most efficient is proof of private key control of an established PIV or CAC. The most common practices a Registration Authority (RA) can leverage for human PIV/CAC holder identity proofing include:

- Mutual TLS authentication such as a web-based registration portal
- Signed S/MIME emails
- Other digitally signed documents (e.g., PDF, Microsoft Office, PureEdge, Lotus documents.)

It is critical to note the difference between electronic signatures and digital signatures, the latter of which is based on proof of control over a private key. Employing digital signatures on forms can be especially useful when a cryptographically signed artifact needs to be transferable and easily auditable. Form signing is also helpful when it comes to other procedural controls that may be consolidated on the same document such as bot account approval workflows.

An organization looking at employing RPA will also want to consider the processes to approve and provision an account associated with a bot. The account creation process may not be relevant to the RA, but the UID or account name associated with the bot and expressed in the resulting certificate will be important to correlate with an individual bot account.

If software form factors are implemented, key generation and exportability is yet another topic of concern to many security professionals. Depending on the certificate issuance software solution available to the RA or the human sponsor, the RA personnel may have to generate a key and Certificate Signing Request (CSR) on behalf of the requestor. If this is the case, the certificate/key combination will need to be delivered to the requestor in a file (e.g., pfx/p12) secured with a password. The associated password should also be provided to the requestor using an out of band method. Alternately, if requestors are capable of generating keys directly on the systems running the RPA software, Deloitte recommended that the Certification Authority mark private keys as **non-exportable** to assist in the traceability of the chain of custody of the bot certificate. Marking private keys as non-exportable will also assist in preventing ‘sharing’ of the bot credential which may affect auditability of the process.

Along the same lines as key exportability, tracking the chain of custody of the private key is also critical. If more than one individual/administrator will have access to the bot’s activities or the private key itself, those individuals should consider also be identified and tracked by the RA, where feasible. If the private key is stored on a smartcard form factor, or higher the employing organization will need to plan for both physical security of the associated crypto module as well as tracking who has knowledge of the key activation information (i.e., PIN/password) in a traceable format (e.g., log, Jira, Service Now).

The final procedural consideration that the RAs will have to account for is the certificate expiration and revocation process. As mentioned previously, it may not be feasible to register bot identities in an identity management system designed for human registrants, and there may be no automated processes available to revoke a bot certificate when an associated human PIV/CAC is revoked. As a result, RAs will have to coordinate carefully with bot administrators to determine the bot’s active timeframe (e.g., 12-month validity), and put processes in place to plan for what occurs with the bot certificate if the human sponsor ever leaves the organization (e.g., reissue bot to new sponsor).

If you or members of your organization would like more information on leading practices for credentialing a bot, or other RPA related topics, please feel free to contact any of the team members listed below.
This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2019 Deloitte Development LLC. All rights reserved.