SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE ACCESS CONTROL COUNCIL WHITE PAPER

Temporary Identity Credentials for Federal Agency Physical Access Control Systems (PACS)

Version 1.0

March 2020

Secure Technology Alliance
191 Clarksville Road
Princeton Junction, NJ 08550

www.securetechnologyalliance.org

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce, and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

The Secure Technology Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Secure Technology Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report. This white paper does not endorse any specific product or service. Product or service references are provided to illustrate the points being made.

Table of Contents

1 Introduction 4
1.1 Purpose of this White Paper 5
1.2 White Paper Audience 5
2 Requirements for Temporary Identity Credentials 7
2.1 Visitor Definition 7
2.2 Vetting Process for Visitors vs. Employees 8
2.3 Employees Who Forget their PIV Cards 9
2.4 Approaches to Use 10
2.4.1 Non-Personalized Re-Useable Card – Linked to User in the PACS 10
2.4.2 Person-Centric Approach 10
3 Authenticatable PKI Credential Solution for Federal PACS 11
3.1 What Is a CIV Card? 11
3.2 Use of CIV Cards as Authentication Credentials 13
3.3 Use of CIV Cards with a PACS 14
3.4 Issuance Process for CIV Cards 14
3.5 Recovering Temporary Credentials 15
4 Conclusion 16
5 Publication Acknowledgements 17

1 Introduction

Homeland Security Presidential Directive 12 (HSPD-12) has been in effect since 2004 and industry and federal stakeholders have successfully met HSPD-12's control objectives with the now ubiquitous Personal Identity Verification (PIV) credential. However, new requirements have arisen over the years that caused expansion of the PIV technical model, its related policies, and its intended uses, such as:

- PIV-Interoperable (PIV-I) credentials
- PIV-Commercial/Commercial Identity Verification (CIV) credentials
- Derived PIV credentials for mobile devices

NIST publication SP 800-116 Rev. 1, "Guidelines for the Use of PIV Credentials in Facility Access," Section 6.5,[1] addresses the technical issues of temporary, interoperable credentials. While SP 800-116 Rev. 1 was first published as guidance, the Office of Management and Budget (OMB) M-19-17 "Enabling Mission Delivery through Improved Identity, Credential, and Access Management,"[2] published in May 2019, made it normative.

Temporary identity credentials that interoperate with the PACS are not a new concept in Federal Government policy. What has not been addressed (nor universally standardized and implemented) are *consistent government-wide policies and models* for issuing and managing short-term, temporary credentials that may be used for access to federal agency facilities, and, potentially, access to federal agency information technology resources. The United States Department of Defense (DoD) came to this same realization in 2014. One of the DoD's physical security policies, "Interim Policy Guidance for DoD Physical Access Control," Attachment 4,[3] makes electronically verifiable credentials the minimum requirement for visitors to any DoD location. The DoD policy states that all PACS must be upgraded (as funding becomes available) to read other agencies' credentials (i.e., PIV), and states further that unescorted visitors without these credentials are to be furnished with "locally produced, temporary issued, visitor identification" that interoperates with the PACS in the same electronic fashion. This document provides guidance for other agencies that may be searching for similar approaches.

Implementation of temporary identity credentials requires the PACS and associated policies and processes to accommodate capabilities for:

- Understanding if a visitor[4] is eligible and approved to gain access to specific physical locations at a particular time of day.
- Authenticating the visitor and the pedigree of the credential being presented, regardless of the issuer.

[1] https://csrc.nist.gov/publications/detail/sp/800-116/rev-1/final

[2] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[3] https://www.cac.mil/Portals/53/Documents/DTM-09-012.pdf

[4] For the purpose of this white paper, the term "visitor" refers to individuals that may not possess a credential that can be used for physical access authentication purposes, or an individual whose existing credential (e.g., PIV card) may not be readily leverageable or available for authentication purposes within a particular PACS. The term "visitor" is defined in more detail in Section 2.1.

- Provisioning the credential with the appropriate access level and start/end date/time for the duration of the visit and no longer. The visitor provisioning process may include personalizing a visually unique badge that includes the visitor name and picture.
- Identifying visitor escort requirements, executing escort workflow, and managing visitor/escort engagement, linking, control and disengagement.
- Maintaining comprehensive detailed activity logs, audit trail, and generate detailed reports.

1.1 Purpose of this White Paper

Modern access control systems used in federal facilities are designed to authenticate and validate high-assurance credentials such as PIV/PIV-I cards and Department of Defense (DoD) Common Access Cards (CACs). The Secure Technology Alliance Access Control Council – which includes both industry and federal government members – developed this white paper to:

- Recommend an approach for implementing temporary identity credentials for physical access control systems (PACS) for federal agencies.
- Show how an agency may efficiently issue short-term temporary identity credentials that are intended only for its own internal local trust.
- Highlight essential access control considerations not currently addressed elsewhere.

1.2 White Paper Audience

This white paper is intended for the following government and industry roles that have a stake in addressing and benefitting from the requirements and recommendations for successfully implementing temporary identity credentials for PACS for Federal agencies:

- **PACS Manufacturers**
  Industry PACS system providers whose PACS products can accommodate reading temporary credentials and authenticating the credential holder, as well as managing the lifecycle of the credential and the identity of the credential holder within the PACS.
- **PACS Administrators**
  Federal agency personnel assigned to configure, operate and maintain PACS installations on a daily basis.
- **Credential Issuers**
  Contracted service providers who can issue temporary (and other) credentials based on accreditation and adherence to standards, policies and processes approved by agency personnel responsible for overseeing credential issuance.
- **On-Site Personnel**
  On-the-ground federal-agency personnel (e.g., sponsors, registrars and issuers) who are responsible for daily activities to ensure that individuals are eligible to receive a temporary credential, and who follow the processes for issuing a temporary credential to the individual, as needed.
- **Agency PACS Business/System Owners**
  Federal agency personnel who are responsible for overseeing the implementation and operation of PACS according to defined policies and procedures.
- **Agency HSPD-12 Program Management Office (PMO) Personnel**
  Federal employees and contractors within an agency's HSPD-12/identity, credential and access

management (ICAM) program management office who ensure that HSPD-12-related initiatives and projects are implemented and operated according to defined policies and procedures, and who also are instrumental in procuring compliant and accredited PACS.

2 Requirements for Temporary Identity Credentials

HSPD-12 and the supporting NIST publications only address some of the populations requiring access to certain government facilities. Furthermore, they only address authentication, which is only one element involved in access control. Authorization, administration, audits and accountability are other key aspects of access control. This white paper focuses on providing guidance on authorization – i.e., access privileges assigned to an individual – and briefly describes the other key aspects.

Physical access control is the provisioning of controlled ingress and egress through an otherwise secure perimeter of a designated volumetric space. A PACS – the system – must support the security of the protected space; this includes consideration of travel into and between secured areas for all members of the population that have a justification to be in the protected space.

PACS need to be able to handle visitors with a site-specific orientation. Policies must be established for visitor management that consider:

- Access by government employees who are not required to have a PIV card.
- Access by government employees from another agency who are not registered in the site PACS.
- Access by non-government employees who require access to designated protected spaces.
- Pre-determination of authorization levels for protected spaces.
- Registration of validated PIV cards and site-specific tokens for visitor use, with a process that restricts access to designated protected spaces.
- Escort requirements.

2.1 Visitor Definition

The term "visitor" has a broad definition. A visitor is someone who meets either of the following criteria:

1. Does not possess a credential that can be provisioned into the PACS but is approved for access on a temporary basis.
2. Possesses a credential that can be provisioned into the PACS but has an access grant that expires before the credential does (e.g., has a PIV credential but is not authorized for perpetual access).

The following are examples of visitor categories that meet these criteria, each with its own unique considerations and policies:

1. **Internal visitor:**
    a. The visitor is from same agency/organization but is based at another location (i.e., is not registered in the building PACS). The visitor has a PIV credential.
    b. A person who forgot their PIV card. The person looks just like a visitor unable to electronically verify their identity to the PACS.
    c. A person who lost their PIV card, or had their card stolen
2. **Other government agency (OGA) visitor**: The visitor is from another agency and has a PIV credential from that other agency.

3. **External visitor:** Contractor or other visitor who has a PIV-I card.
4. **Short-term visito**r: Visitor without a PIV/PIV-I card or CAC (for whatever reason) who needs a temporary identity card (e.g., for use for one day to four weeks).[5] These visitors may fall into a number of subcategories:
    a. Escort required
    b. No escort
    c. Contractor – escort
    d. Contractor – no escort
    e. Employee – no escort
    f. VIP – no escort
5. **Longer-term visitor:** Visitor without a PIV/PIV-I card or CAC who needs a personalized (i.e., with a photo) temporary identity card (e.g., for use from one to six months).[6] These visitors may fall into a number of subcategories:
    a. Escort required
    b. No escort
    c. Contractor – escort
    d. Contractor – no escort
    e. Employee – no escort
    f. VIP – no escort

2.2 Vetting Process for Visitors vs. Employees

The following are examples of vetting considerations/processes that include the range of visitors defined in the previous section.

Process of Vetting Personnel

- Vetting for visitors (visit duration of one to 30 days): This process provides personnel who may want to visit an agency site with temporary access to restricted locations within the facility/site. Visitors should generally present one form of identification (e.g., for name match verification).
- Card issuance: The card issuance process establishes the application/use of the card being issued to the individual (e.g., building access, computer access, site recognition by employees) for the facility that the individual is visiting, with emergency contact information available in case of emergencies.

Process of Vetting Foreign Personnel

Each agency has its own policies for vetting visitors from foreign nations, and the policies vary greatly. Foreign visitors are usually escorted by their host; this document only mentions a few common considerations.

- Proper vetting of foreign personnel is critical to securing the site/facility to information/equipment being seen by unauthorized foreign entities.

[5] Note that the temporary identity credentials may be preprinted and work with readers supporting up to two factors.

[6] Picture on topology and supporting up to three-factor readers.

- Vetting foreign nationals should be reviewed and appropriately approved. Issued credentials should be based upon appropriate approvals and access to the site/facility. Physical access control privileges should be modified accordingly by approval.

2.3 Employees Who Forget their PIV Cards

Employees who do not have their primary credentials (i.e., PIV cards) need to have their identity established and their vetted identity bound to and issued on a temporary credential that interoperates with the PACS, if they are to be granted compliant, legitimate access for a period of time. Re-establishing the identity of someone claiming to be an employee presents a significant security risk, since the HSPD-12 and FIPS 201 proofing and vetting processes are not available. Duplicating those processes is impractical for temporary access.

Instead, agencies should use information they have at their disposal to confirm identity. Information commonly available with which to corroborate the identity of someone claiming to be an employee includes:

- The name in the identity management system (IDMS) matches a government-issued ID in the individual's possession.
- The name in the PACS matches a government-issued ID in the individual's possession.
- The photo in the IDMS matches the individual's physical appearance.
- The photo in the PACS matches the individual's physical appearance.
- The individual is able to state the role, office location or other identifying information as recorded in the IDMS.
- The individual's manager of record in the IDMS can be contacted to further corroborate identity.
- The individual can prove possession of an agency email account on a mobile device.

Two critical steps which must be taken when issuing a second credential to an employee:

- Agencies should not allow two credentials to be active at the same time. The primary credential is disabled in each PACS instance to which it has been provisioned. The temporary credential should be associated with that employee's record in the PACS so that access levels/clearance levels are maintained. When the individual shows possession of the primary credential, this process should be reversed.
- Agencies should monitor the length of time that an employee uses a temporary credential. While misplacing a credential or forgetting to bring it to work is common, this situation should not persist for multiple days. If it does, it may be an indication that the employee is no longer in control of the primary credential. A lost credential is the main criteria for PIV credential revocation. Lost credentials have historically been a weakness in high assurance credential programs and represent a significant opportunity to improve security overall. Agencies should create their own policies, but a best practice could be that employees needing to use a temporary credential for more than three days must have their PIV credentials revoked.

2.4 Approaches to Use

2.4.1 Non-Personalized Re-Useable Card – Linked to User in the PACS

An agency may decide on an approach that uses a number of non-personalized public key infrastructure (PKI) credentials (such as CIV card), signed by their own internal root certificate authority that is used specifically for enabling local trust in temporary identity credentials. A non-personalized temporary card is a card that may be issued to a visitor, returned and reissued again to a different visitor without having the visitor name encoded in the card and without requiring a digital signature from the issuer each time it is issued.

To enable technical operation in a PIV environment, where the first and last name data objects in the card must be populated, a reusable card may have these populated and signed with generic fill data (such as Visitor One, Visitor Two, Visitor Three) as the first and last name.

The following describes one option for the issuance process. The visitor center operator picks one of the visitor cards (e.g., Visitor Two). The operator locates the Visitor Two user record in the access control system, changes the user name in the system database to the name of the visitor who will receive the card, and assigns the appropriate access authority and the end date of the visit. This would be done in the access control system, not on the card, simplifying the issuance process.

At the end of the visit, the card is returned to the visitor center. The operator removes the name of the person who used the card from the access control system and returns the no access level to the user record.

This approach is easy and convenient. However, the access control system has a few specific requirements. The access control system must generate a permanent access transaction log that includes recording and saving the name of each person who used the card during a visit. Since some systems use a relationship between the card identifier and the current user name, this requirement may cause issues and indicate that a current visitor used the card for access when, in fact, one of the previous visitors used the card.

2.4.2 Person-Centric Approach

With this approach, the visitor system creates a record for the person, then binds that information to a temporary credential number and pushes it to the PACS. Once the visit is complete, the visitor system removes the credential from the PACS but retains the person and transaction information for auditing purposes. If the same person visits again, a new credential is added to the person record and the new access transactions are added to the person record. This method also allows a temporary credential to be assigned to permanent personnel who may have forgotten their credentials.

3 Authenticatable PKI Credential Solution for Federal PACS

Visitors are authenticated by what they possess, their credentials. The goal of a high assurance PACS is to verify a visitor by validating a credential already in their possession thereby leveraging the identity vetting process that has already taken place. As high assurance credentials become commonplace, this process will become the status quo. However, for the foreseeable future, facility owners will need to interact with a number of different use cases and credentials.

Four credential use cases are currently associated with visitor management in the federal enterprise:

1. "Native"-agency-issued PIV card/CAC (i.e., the facility is the same agency that issued the credential)
2. Other-agency-issued PIV card/CAC
3. Non-federally or federally-issued PIV-I card
4. Locally-issued PIV-C card (i.e., CIV card)
   a. Non-personalized, reusable "building badges"
   b. Personalized, non-reusable "person badges"

This section focuses on the locally issued CIV card as the solution.

3.1 What Is a CIV Card?

A Commercial Identity Verification (CIV) card[7] is an authentication token that uses a smart card form factor technically comparable to a PIV or PIV-I card. The CIV credential was originally intended for commercial organizations that were seeking a credential for use for their employees, subcontractors, nonemployee visitors and customers. In that original context, the CIV card is equally suitable as an authentication platform that can be leveraged for agency use as a temporary credential.

The reasons why a CIV credential is identified in this white paper as the candidate for a temporary visitor credential include:

1. **Flexible Policies and Processes**. A CIV card can be a less expensive alternative to PIV or PIV-I cards since there are fewer policy and process compliance requirements for a CIV credential than there are for a PIV/PIV-I credential. That is, agencies can specify their own CIV vetting, identity proofing and issuance policies and procedures that suit their agency-specific needs to accommodate visitor access to agency facilities and resources.
2. **Proven Technology**. The CIV credential is based on the proven PIV/PIV-I credential technical model that establishes very strong authentication.

A short comparison of the policies, process, and technologies for the CIV credential model versus the PIV/PIV-I credential model is included in Table 1.

[7] For more information on the CIV credential, see the Secure Technology Alliance white papers, "The Commercial Identity Verification (CIV) Credential Leveraging FIPS 201 and the PIV Specifications" and "A Comparison of PIV, PIV-I and CIV Credentials" at https://www.securetechalliance.org/publications-the-commercial-identity-verification-civ-credential-leveraging-fips-201-and-the-piv-specifications/.

Table 1. Comparison of CIV Credentials with PIV and PIV-I Credentials

	PIV	PIV-I	CIV
Vetting and Identity Proofing Policies	FIPS 201	FIPS 201	Issuing organization defined policies
Background Checks Policies	NAC-I	Issuing organization policies	Issuing organization defined policies
Processes (e.g.,Sponsorship, Adjudication, Enrollment, Issuance)	FIPS 201	Based on FIPS 201	Issuing organization defined processes
Card Data Model	NIST SP-800-73	NIST SP-800-73	NIST SP-800-73 recommended but not all data elements are mandatory
Primary Credential Identifier	FASC-N and/or Card UUID	Card UUID	Card UUID
Certificate Authority	Federal Bridge	Cross-certified to the Federal Bridge	Issuing organization trusted local or external certificate authority

To be used in a federal agency, the CIV card would use a PIV applet that is listed on the FIPS 201 Approved Products List.[8] The PIV application on the CIV card is populated with data elements that are compliant with the data model defined for PIV and PIV-I cards (as specified in NIST SP 800-73, SP 800-76 and SP 800-78), but not all of the data elements are necessarily mandated to be populated for the CIV credential.

The CIV card description in this white paper has been carefully written to describe the flexibility that the CIV credential is intended to provide without referring to the "must/normative" requirements, policies and/or standards that apply to PIV and PIV-I credentials. The CIV credential is neither tightly defined nor specified. Several CIV cards are already commercially available with some marketed under other brand names.

This lack of specificity, which is a major hindrance to interoperability, is precisely because the CIV credential is not intended to be interoperable across agencies. Instead, use of the CIV credential is for local trust and local use cases. This approach is manifested in three ways:

1. The CIV credential can be issued without the burden of cross-certification to the Federal Bridge and can be anything that the issuer wants since the issuer knows what the credential will be used for, and importantly, what it will not be used for.
2. The CIV credential is not certified by a trust broker to be part of a trust framework. Specifically, the CIV credential does not contain policy object identifiers (OIDs) that would cause an access control system to believe that the credential could be validated through the Federal Bridge as a

[8] https://www.idmanagement.gov/approved-products-list-piv/

PIV or PIV-I credential. Issuers of CIV credentials are concerned with a local trust use case. Simply put, a local trust use case does not require the external trust capability afforded by Federal-Bridge-backed credentials.

3. A federal or commercial CIV credential issuer may create their own identity vetting policies, issuance policies and trust anchor (certificates) without the expense of cross certification to the Federal Bridge.

Interoperability aside, it may benefit the federal government to recommend common CIV technical requirements for CIV temporary cards, such that PACS vendors and CIV card issuers only have to implement configurations and profiles once for CIV card issuance and CIV card authentication. Otherwise, agencies would have to pay for PACS and CIV card issuance customizations individually, rather than leverage pre-existing configurations and profiles that PACS vendors and CIV card issuers may have already implemented using a common technical model.

3.2 Use of CIV Cards as Authentication Credentials

An authenticatable credential, as its name suggests, is a token capable of being electronically authenticated and validated as genuine and unaltered. However, not all tokens have the same capabilities. Three terms help to identify these differences. (Note that the examples below are based on PKI digital certificate credentials.)

- **Identification** – provides a credential identifier. A credential can be identified without being authenticated and/or validated. As an example, CIV cards may have a Chip Serial Number (CSN), a Federal Agency Smart Credential Number (FASC-N), and/or Card Unique Identifier (CUID) that are freely readable unique identifiers. Reading these numbers will identify the card but will not provide assurance the credential is genuine or unaltered.
- **Authentication** – provides minimal assurance the credential is genuine and unaltered. Optionally, authentication can also give assurance that the credential holder is who they claim to be. As an example, CIV cards would contain a Card Authentication Key (CAK) certificate and corresponding private key for use in physical access scenarios. Authenticating the credential by doing a challenge/response transaction with the CAK, and verifying the signatures of the signed data elements on the card used for identification will provide assurance the credential is genuine and unaltered, but will not validate the binding between the credential and the credential holder. If the PIV Authentication Key (PAK) certificate and corresponding private key are present on a CIV, use of the PAK will provide some assurance of the credential holder's identity since a PIN is required to enable cryptographic functions for the PAK. The PIN provides a "what you know" factor of authentication; if the entered PIN is compared to a reference PIN stored on the card (as opposed to a PIN stored in a PACS database) assurance of the binding between credential holder and credential is obtained.
- **Validation** – provides assurance the credential is in good standing to be used for authentication at that moment. Validity, in this context, is temporal. Authenticating a credential based on PKI only gives assurance that the credential may have been issued by a trusted CA. Authentication, by itself, does not provide assurance that the credential is still trustworthy, nor that the credential is still valid according to that CA. Validation provides real-time assurance that a card is still in good standing, much like a credit card is validated online at a point-of-sale terminal with the credit card issuer. For example, PIV and PIV-I credentials rely on Path Discovery and Validation (PDVAL), which uses the Federal Bridge to provide assurance that the digital certificates (e.g., CAK or PAK digital certificates) stored on the card are still in good standing;

e.g., not terminated or revoked. Once the CA's current trustworthiness has been established, asking the CA to provide status about the individual credential is safe to do. This process is most commonly done via the Online Certificate Status Protocol (OCSP) or use of downloaded Certificate Revocation Lists (CRLs). Because CIV credentials are only trusted locally by the issuer, access control systems relying on CIV credentials should do a revocation check using the local CIV card issuer trust anchors.

3.3 Use of CIV Cards with a PACS

When a CIV card is presented to a smart card reader (either ISO/IEC 7816 contact or ISO/IEC 14443 contactless), the card responds like a PIV-I card and has the following characteristics:

- The card contains a PIV applet.
- The card's PIV applet has all of the required containers/structures defined by NIST SP 800-73. The CIV credential does not mandate any specific data be populated in any container. Additional containers outside of the PIV data model are optional and issuer dependent.
- For a CIV card to be used in a federal PACS, the card identifier in the CHUID (and the other structures) must be encoded with the Card Universally Unique Identifier (CUUID). The FASC-N fields for Agency Code – System Code - Credential Number in the CHUID shall be all 9s (9999-9999-999999). All other FASC-N fields may be populated in accordance with the CIV credential issuer requirements and issuance practices.
- The digitally signed card data objects, as well as the cryptographic functions for all PIV-specified containers, shall be compliant with NIST SP 800-78. Additional containers are out of scope of this requirement.
- Any biometric information stored on the card in a PIV-specified container shall be compliant with NIST SP 800-76.

3.4 Issuance Process for CIV Cards

NIST SP 800-116 R1 states that electronically verifiable cards should be used for visitors who do not already have a suitable credential. No federal policy explicitly states how CIV credentials should be issued to visitors. Agencies and sites are likely to establish their own standard operating procedures that take their risk posture into account when issuing temporary credentials. The following three main areas should be considered:

1. **Visitor Identity Proofing**. For visitor identity proofing, a PIV card or CAC is not available, so some other proof of identity is necessary. The most common ID credentials held in the general population are driver's licenses and passports. REAL ID-compliant driver's licenses are likely to be the most common proof of identity. Referring to NIST SP 800-63-3, as state departments of motor vehicles bring their REAL ID systems online, agencies who rely on driver's licenses as a primary proof of identity should use automated systems to validate the document in order to achieve a much higher level of assurance for visitor identity. For higher security facilities, additional identity assurance can be gained by using fraudulent document detection technology. Those facilities that choose to accept passports should be able to do similar, technology-based document verification for those as well.
2. **Visitor Identity Vetting/Suitability**. Some facilities may need to have visitor background information. Agencies who use an electronic visitor management system may find varying degrees of automation and support for doing this in a repeatable way. The critical element is

having a system that acts as the source of authority for the user identity that tightly couples the identity proofing, the identity vetting results, and the temporary credential that will be issued to the visitor. Vetting may also include accessing public records and other online repositories and/or services that may expose undesirable activities that the candidate visitor may have been engaged in.

3. **Temporary Credential Binding**. NIST SP 800-116-1 recommends that agencies should consider the performance, costs, and security tradeoffs between using disposable versus reusable temporary credentials/badges for physical access scenarios. Using reusable/disposable temporary credentials means that the credential/card is inherently and originally unbound to a specific individual. Providing personalized cards to all visitors is more expensive and time consuming than using non-personalized reusable cards. The ideal situation is to balance security and cost, while having the flexibility to provide different types of credentials based on facility and visitor type requirements. Using personalized, and perhaps disposable, cards is straight forward – as that is the basis of most PACS and visitor management system implementations. Reusable cards are beneficial in that it reduces the need for consumable stock, as long as the PACS and/or visitor management system can accommodate, bind, and track reusable cards as they are assigned and unassigned from one visitor to another.

3.5 Recovering Temporary Credentials

It is a common misconception that a CIV credential (or any credential) that leaves an agency in an unauthorized manner can no longer be trusted upon its eventual return. However, a visitor inadvertently, or even on purpose, leaving with a CIV card need not be a security concern. If the visitor management system is appropriately provisioning facility access privileges to the PACS for just the duration of the visit, a departed card introduces no security risk. The card will have no access rights in the PACS as long as personnel managing the PACS deprovisions the card from the PACS database.

However, departed cards can have a significant impact on the total cost of visitor management. Several good technological and process solutions are available to ensure timely return of the temporary card. Solutions range from a lobby ambassador (whose job is to interact with all departing visitors to request the return of the credential) to facility egress points where visitor cannot physically leave unless the card is returned.

For organizations that are operating at the highest security postures, CIV cards may be added to a revocation list which puts their digital-certificate serial numbers on the CRL published by the certificate issuing CA. While the card should never have any residual access rights in the PACS, being put on the revocation list would act as a fail-safe measure. Should the card ever be returned, depending on the specific PKI technology used, it may be possible to remove the card from the revocation list, effectively entering it back into service. It is important to remember that the security mechanisms built into FIPS 201-approved cards and the NIST Personal Identity Verification Program (NVIVP)-approved PIV applets are sufficient to detect any tampering and would render the card useless.

4 Conclusion

Temporary access cards that are vendor-agnostic and compatible with modern, GSA FIPS 201 APL access control systems may be created and issued in accordance with local agency policies and are commercially available from several manufacturers. The PKI-based CIV cards described in this white paper are resistant to unauthorized modification, counterfeiting and cloning and may be authenticated electronically.

The CIV card can work effectively as a visitor credential where the local PACS is fully compliant with the current GSA FIPS 201 Evaluation Program specifications.

5 Publication Acknowledgements

This guidance document was developed by the Secure Technology Alliance Access Control Council to to outline the requirements and discuss a solution for issuing and using temporary identity credentials for federal agencies.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Secure Technology Alliance thanks the Council members for their contributions. Participants involved in the development of the white paper included: CertiPath; G+D Mobile Security; GSA; HID Global; ID Technology Partners; IDEMIA; Identiv; Integrated Security Technologies; IQ Devices; Parsons; Secure Element Solutions; SigNet Technologies, Inc.; Tyco Software House; Veridt, Inc.; XTec, Inc.

Special thanks go to **Lars Suneborn**, ID Technology Partners, who managed the project.

The Secure Technology Alliance thanks the following Council members who contributed to writing and/or reviewing the white paper, including:

- **Mark Allen**, Identiv
- **Mark Dale**, XTec, Inc.
- **Tony Damalas**, SigNet Technologies, Inc.
- **Tina Davis**, CertiPath
- **Mark Depp**, Veridt
- **Jatin Deshpande**, G+D Mobile Security
- **Clay Estes**, HID Global
- **Christophe Goyet**, IDEMIA
- **Daryl Hendricks**, GSA
- **Mike Kelley**, Parsons
- **Gilles Lisimaque**, ID Technology Partners
- **Stafford Mahfouz**, Tyco Software House
- **Cathy Medich**, Secure Technology Alliance
- **Dan Myslewski**, CertiPath
- **Jeff Nigriny**, CertiPath
- **Paul Retzbach**, CertiPath
- **Roger Roehr**, Integrated Security Technologies
- **Devon Rohrer**, Secure Technology Alliance
- **Steve Rogers**, IQ Devices
- **Gerry Smith**, ID Technology Partners
- **Lars Suneborn**, ID Technology Partners
- **John Watson**
- **Mike White**, IDEMIA
- **Mike Zercher**, Secure Element Solutions
- **Rob Zivney**, ID Technology Partners

Trademark Notice