

# ***National Strategy for Secure Online Transactions (NS-SOT)***

## **Information Card Foundation Response**

### ***Introduction***

This document has been prepared in response to a request for input by Ely Kahn and Deloitte & Touche staff in a meeting held during the RSA conference on 2 March 2010 and attended by members of the Information Card Foundation (ICF) board of directors.

The ICF and its member companies believe that the formulation of a National Strategy for Secure Online Transactions is an outstanding opportunity to extend the public/private partnership that the ICF, the OpenID Foundation (OIDF), and the Open Identity Exchange (OIX) have developed with the federal government over the past year. Specifically, we believe that the Federal Identity, Credentialing, and Access Management subcommittee (Federal ICAM or FICAM) trust framework program, announced last September, together with the recent announcement of OIX as a FICAM-approved trust framework provider, is an opportunity for the government to step fully into three leadership roles in the adoption of secure online transactions:

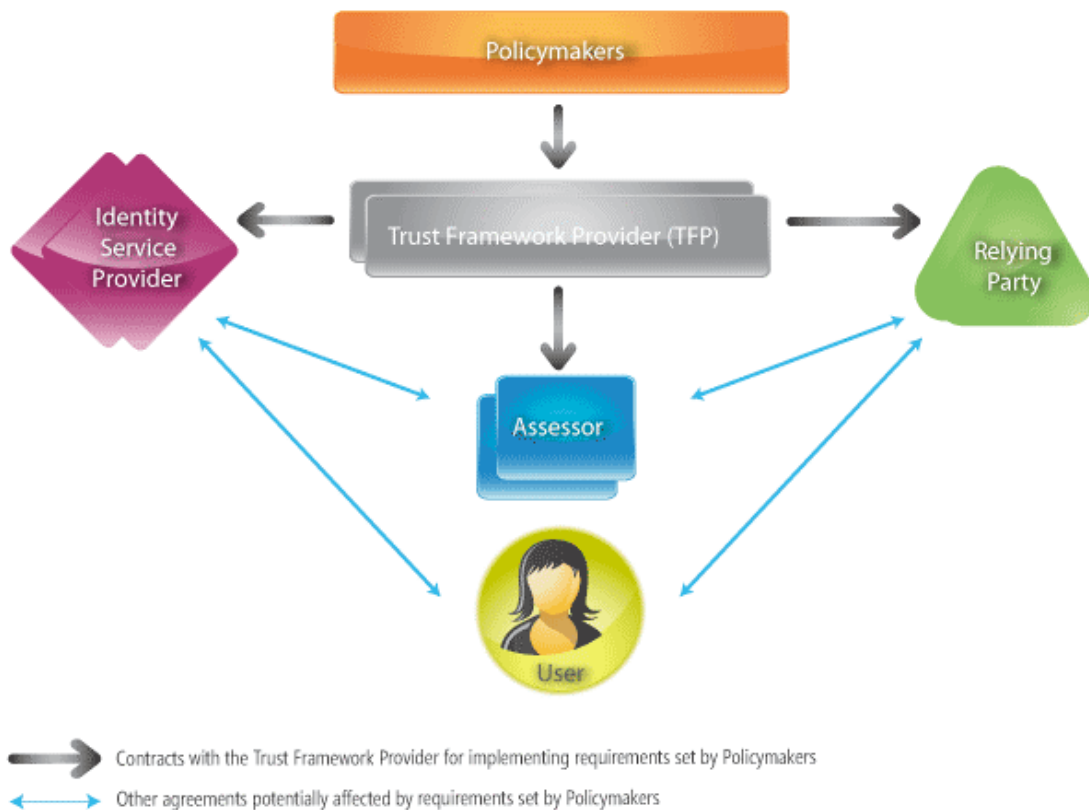
1. To serve as the **Enabler** for trusted government services, by continuing to adopt policies that support the FICAM trust framework;
2. To be an **Early Adopter** of the Open Identity Trust Framework model, using the federal government's scale as the "world's largest service provider", to aggressively begin to offer trusted online services to hundreds of millions of people; and
3. To be the **Defender** of the Open Identity Trust Framework ecosystem in the same way that the federal government has defended and protected the previous critical components that supported our economy and social institutions.

At first the ideas in this document might be perceived of as being overly tactical, or worse, yet another appeal for a government handout. But the reality is quite different. In working with FICAM to this point it is clear that the key issues that would thwart any national strategy for secure online transactions are not technological in nature. The technology problems have been, to a large extent, solved by industry and are continuing to be addressed in a broadly supported, open-standard approach that can scale globally (like the Internet itself). Rather, the key remaining issues are those that relate to business models, regulatory protections and constraints, and implementation dependencies. All of these can be addressed strategically, but ultimately require tactical action. A vague or conceptual "strategy" that results in unfunded mandates to agencies operating independently will not advance the cause of secure online transactions, and may cause more damage to the effort than doing nothing at all.

## The Open Identity Trust Framework Model

Before we move to specific recommendations, we should emphasize that all of these fit within the identity, security, and privacy model developed over the last year in the partnership between FICAM and industry as represented by ICF, OIDF, and OIX. This Open Identity Trust Framework (OITF) Model is documented in a white paper of the same name [1] published by all three of the foundations.

This model for the delivery of trusted services not just within the U.S. but across the Internet as a whole is captured in the following diagram of the open identity ecosystem.



The fundamental rationale behind this model is to harness commercially available off the shelf solutions (COTS) to provide the identity, security, and privacy assurance needed for many-to-many trust relationships on the Internet. The key advantages of this approach are:

1. Different trust frameworks can serve different identity, security, and privacy requirements for different trust communities – it does not force "one size fits all".
2. Each trust framework can define the levels of assurance (LOA) and levels of protection (LOP) that best map to their requirements.
3. Each trust framework can also specify the open identity technology profiles (e.g., OpenID, Information Cards, SAML, WS-Fed) that best meets their needs (as FICAM has already done with the IMI 1.0 and OpenID 2.0 Profiles).

4. An open market helps insure competition, innovation, and pricing pressure for identity provider and assessor services.
5. This model can evolve and adapt as both technology and policy change.
6. In all areas this model gives consumers choice, control, and confidence.

The development of this model has been a major step forward for both government and the open identity industry. It represents an unprecedented level of consensus about how to build trust in transactions in an environment as diverse as the Internet. We therefore suggest it should be the backbone of the NS-SOT. It is also the backbone of the following recommendations.

## ***Specific Recommendations***

The following strategy suggestions are designed to work *with* the complexities of the entire ecosystem as captured in the OITF model, not to control it. It is crucial that we leave flexibility for continued innovation in this space if we want to see continued improvements in security and assurance.

Thus, instead of a top-down strategy that would purport to be a "new" government approach, we propose a series of targeted interventions by government to catalyze desired responses from the broader ecosystem. In this regard, we believe that all aspects of the proposed approach are important, and interconnected. The financial investments proposed are modest in scale and catalytic in intent. They are not intended to be sustaining nor permanent.

The combined experience of dozens of our member firms informs these recommendations and gives us confidence in the proposed approach and its specific recommendations.

### **I. Immediately Secure Government-to-Citizen Transactions**

With the adoption of the OITF model, and the recent certification of the initial identity providers for OpenID and IMI Information Cards to the FICAM trust framework requirements, the Federal government is now positioned to move forward with securing government-to-citizen interactions on its own websites at LOA 1.

Whereas, the overall NS-SOT will ultimately embrace a broader set of scenarios (including B2B, B2C, etc.), we suggest the strategy should initially focus on online Government-to-Citizen service delivery. The rationale is as follows:

1. This is an area where the federal government can play a **catalytic role** as a early adopter and buyer. Government agencies can issue RFPs that require open identity technologies (e.g. Information Cards and OpenID) supported by open identity trust frameworks (e.g. Open Identity Exchange and others). Even relatively modest efforts in this direction will rapidly crystallize and stimulate the market, creating the incentive for follow-on commercial investment in this area.
2. We can **improve service delivery to citizens** in ways that tangibly benefit a wide constituency and build good will.
3. Identity management technologies are inherently well suited to **reducing waste** caused by authentication-based fraud, for example where citizens obtain costly benefits to which they are not entitled.

4. The proposed approach builds on and reinforces the administration's **open government** initiatives.
5. The claims-based approach described below **enhances privacy** by transmitting only the minimal set of attributes across the network to the relying party.

This last point above is an opportunity to demonstrate that the NS-SOT initiative can mitigate negative perceptions of the federal government as "big brother." Using open identity trust frameworks enables the US government to accomplish its goal of securing online transactions without resorting to a government-wide "identity card" for citizens and residents. By recommending technologies that protect user privacy the government can avoid much of the fear and resistance engendered by earlier identity-related initiatives such as REAL ID.

## **II. Focus on Government as Early Adopter**

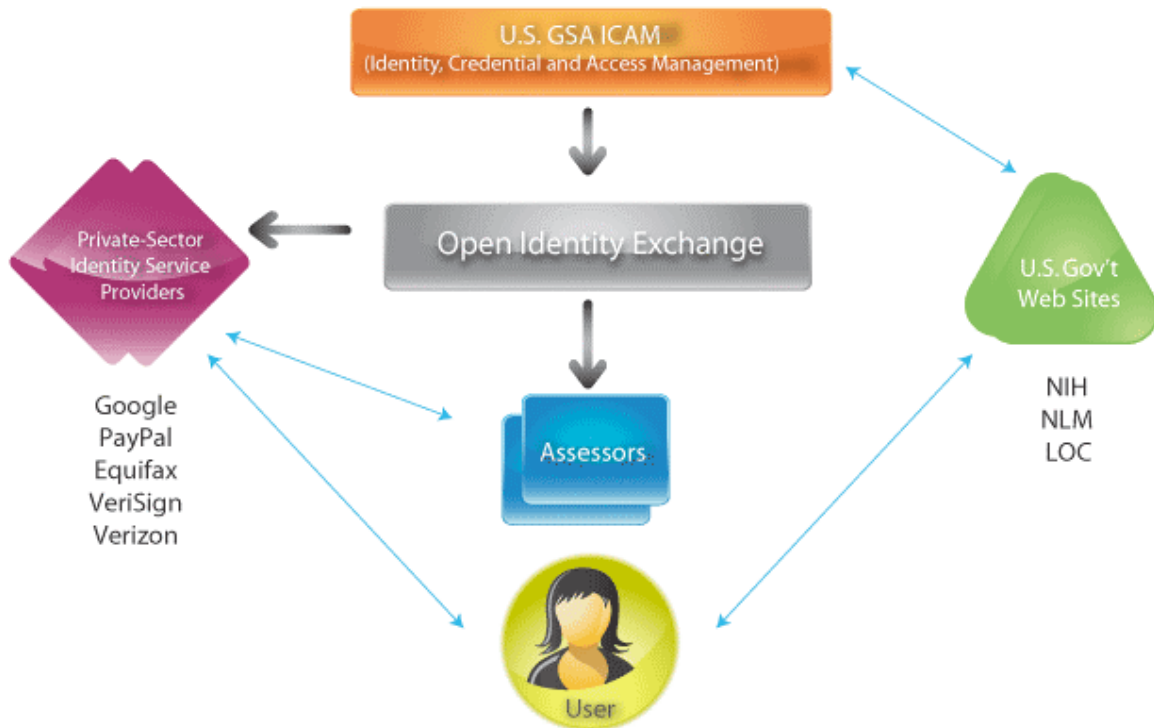
The Federal government must become an early adopter of open identity trust frameworks and open identity technologies in its own online services and applications. This is no longer a question of being the "first mover" and taking unwarranted adoption risks. NIH and GSA have already shown that the technologies work, and with OIX the trust framework is now in place. So proceeding with the early adopter phase must not wait for the FY12 budget cycle. The government should immediately:

1. Enable at least 5 existing services offered by Federal agencies, including at least one with notable exposure and significant citizen facing functions. Ensure that this set includes services whose authentication requirements span NIST levels of assurance 1 through 3
2. Re-use existing trust frameworks (e.g. FICAM) wherever possible. Otherwise, the government should be tasked with defining new ones.
3. Re-use existing Identity Schemes (as FICAM refers to them) wherever possible. Otherwise, again, the government should be tasked with adopting new ones.
4. Provide RFP guidance for Federal government procurements, in particular with all e-authentication, single sign-on, and other identity-related RFPs.
5. Assign \$20 million in current fiscal year funds. Make these funds available to the target agencies to enable them to (i) pay for identity information (claims) provided by commercial identity providers (ii) adapt their existing infrastructure to be compatible with the existing FICAM trust frameworks and identity scheme protocols (i.e., IMI Information Cards 1.0 and OpenID 2.0).

## **III. Focus on Government in the Relying Party Role**

The Federal CIO, Vivek Kundra, recently described the government as having more than 24,000 websites –yet almost none of them have progressed beyond the "brochureware" level when the web was viewed simply as a low cost way to publish information. Today and in the future, citizens expect "service providers" to deliver an increasingly rich set of personalized data, applications, and services to all kinds of devices and networks. Government websites have not been able to keep pace with what is expected by the rest of the market. As a result, it costs the government more than it should to deliver services, and the service experience isn't up to commercial standards.

In the OITF ecosystem, the FICAM trust framework has a specific configuration that is shown in the diagram below.



In this configuration, it is the responsibility of the government to ensure that government relying party websites are compliant with FICAM requirements and can accept and process credentials from FICAM-compliant identity providers.

It is critical that the government move forward with doing this with a reasonable cross-section of U.S. federal agency websites as quickly as possible. This will provide tangible proof of how the Open Identity Trust Framework approach can streamline registration for online services and simplify the login and authentication process for users, while at the same time improving the overall security of the online experience. It will allow the government to begin to operate as a true "service provider" to its citizens.

Adoption of the FICAM trust framework (initially for services requiring LOA 1 credentials) will allow the government to transform its operations, lowering costs and improving services in compliance with the Administration's Open Government Initiative. This should become an immediate priority of the National Strategy for Secure Online Transactions.

The government should also move aggressively to take advantage of the OITF model to reduce costs – and fraud – across higher value services that require authentication using NIST Level 2, 3, or 4 credentials. Even though the FICAM trust framework has been adopted as part of the Federal Enterprise Architecture, the government has yet to take any specific action to fund or mandate its adoption. As a result, it is missing the opportunity to achieve many of the Open Government Initiative's goals.

Some examples that illustrate both the opportunity and the opportunity costs:

- The Department of Homeland Security operates a database of more than 2 Million "First Responders" who must be relied on in cases of national emergency. Even though there are systems to register these individuals, the government still plans on issuing its own credentials to these individuals rather than allowing them to use third-party credentials. As a result, services are being delayed, and many in this community cannot interact as efficiently as they could with third-party credentials.
- The Centers For Disease Control (CDC) operates a wide variety of clinical trials in which physicians need to share data on the results. Today, these physicians are asked to establish their credentials by filling out physical forms in front of a local notary public and to then mail them into the CDC for processing. This costs the physicians time and money and results in far lower participation than if physicians could use third-party credentials through the FICAM trust framework.
- The IRS today offers very few interactive services through its online portal. At the same time the agency is now being asked to certify many thousands of tax preparers, although it has no online authentication model in place. Theoretically, the IRS will issue its own credentials – at added expense – rather than use third-party credentials. Moreover, under the current plan for Health Reform, the IRS will also become the "processing agent" for what is estimate to be as many as 30 Million additional filings per month, yet it has no current plans to use online capabilities to support this additional demand.
- In the overlap of federal programs, there are many instances where a person is allowed to obtain benefits only through one program or another. Likewise, many programs suffer huge losses as the result of identity fraud and fraudulent filings. These could be avoided with better user authentication. Commercial enterprises have long recognized cost savings and fraud reduction by moving service application and delivery to online systems where identity can be verified and tracked. Using the FICAM trust framework to enable broad transformation of existing service models to efficient online authentication models can significantly reduce costs and fraud.

Even though there will be a cost to the federal government for the use of third-party credentials above LOA 1, this cost will be far less than what the government is actually incurring now by not offering truly interactive services to its citizens. Any cost from third-party credentials will be insignificant when evaluated against the cost savings enjoyed, the operational benefits derived, and the reduction in fraud, particularly when the cost is spread over millions of online users and more than 24,000 US government websites.

#### **IV. Maintain Authentication Technology Neutrality**

Authentication technologies (e.g. biometrics, smart cards, passwords, et al) should be considered "plug-ins" to the online identity management layer. While online identity management architecture *requires* authentication and credentialing, the architecture can and should be designed to accomodate a wide variety of authentication technologies as well as be adapted to new ones yet to be developed. As a consequence the NS-SOT should be neutral with regard to authentication method.

## **V. Maintain Token Neutrality**

The "meta" in the term "identity metasystem" refers primarily to the fact that the architecture is "token neutral". This means the same system can deal with multiple token types, from SAML tokens to Kerberos tokens to OpenID tokens.

The NS-SOT should take this same architectural approach because it enables the use of less expensive light-weight technologies (e.g., OpenID) where they are adequate, while also supporting heavier-weight (more secure) technologies (e.g., Information Cards with SAML tokens secured by hard tokens) where necessary.

It also means that token-neutral protocols such as IMI 1.0 Information Cards can support innovative new token types such as the U-Prove token recently announced at RSA. As described by Microsoft, "U-Prove is an innovative cryptographic technology that enables the issuance and presentation of cryptographically protected claims in a manner that provides multi-party security." This user-centric technology is just the most recent example of the type of secure, privacy enhancing technology that can be delivered using the Open Identity Trust Framework model.

Extensibility is also important because in any large rollout it will be necessary to continue support for legacy authentication methods for differing lengths of time. This enables agencies to gradually phase out username/password in favor of more secure and privacy protecting authentication and data sharing technologies.

## **VI. Migrate from Identifiers to Claims**

Although the ability to reliably identify real people by digital identifiers (e.g. a person's name, SSN, employee number, etc.) is crucial for many use cases (including law enforcement and national security), there are many others where attributes *other than an identifier* are also needed. In yet other cases only these non-identifying attributes are needed, and no privacy-invading identifier is required at all. For example an attribute might indicate a role, rank, or authorization level. It is often best to present a highly specific authorization (e.g. the ability to access a specific class of resource (e.g. a digital artifact or service) attribute.

For these reasons the modern identity protocols have moved to a "claims-based" foundation. Open identity technologies (e.g. Information Card and OpenID) are claims-based and can reliably convey an arbitrary set of attributes to a relying party. And since identifiers are just special kinds of attributes, clearly this approach can also convey identifiers. The result is a way to deliver more personalized services and more robust systems that are also maximally privacy protecting.

## **VII. Take Leadership on Levels of Protection (LOP)**

Lastly, beyond mandating and leading adoption of open identity technologies and open identity trust frameworks, the government also has the opportunity in the NS-SOT strategy to lead in establishing a precedent for trust frameworks to include Levels of Protection (LOP) in addition to Levels of Assurance (LOA).

To some extent this had already started: the existing FICAM trust framework already specifies a set of government privacy standards to which industry identity providers must conform in order to be certified. However, as currently formulated, the FICAM

trust framework does not mandate conformance by government websites acting as relying parties.

It would be advantageous if FICAM had a clear mechanism for specifying and certifying that federal websites serving as relying parties are appropriately protecting the identity and claims information that they receive about users via the FICAM trust framework.

This could be done by having the next versions of the FICAM trust framework specifications incorporate the concept of LOP, and specify the LOP appropriate for handling certain types of personally identifying information (PII) for certain types of citizen-government transactions. Furthermore, certification of the LOP achieved by government websites could increase user confidence that personal data is being treated properly.

Finally, support for LOP by the Federal government would create a precedent for industry to follow. This would spur the adoption of trusted services and user-centered protections beyond government, increasing the overall security of information technology infrastructure in the United States.

## ***References***

[1] Open Identity Trust Framework (OITF) Model,  
<http://www.openidentityexchange.org/sites/default/files/the-open-identity-trust-framework-model-2010-03.pdf>