Blended Identity: Pervasive IdM for Continuous Authentication

Patricia Arias-Cabarcos[1], Florina Almenárez[1], Rubén Trapero[2], Daniel Díaz-Sánchez[1], Andrés Marín[1]
[1]Telematic Engineering Department, University Carlos III of Madrid
Avda.de la Universidad 30, 28911, Leganés, Madrid, Spain
Phones: +34 916246237, +34 916248799, +34 916246233, +34 91624629947
Fax: +34 916248749
{ariasp, florina, dds, amarin}@it.uc3m.es
[2]Department of Computer Science, Technische Universität Darmstadt
Hochschulstr. 10, Piloty Building, 64289, Darmstadt, Germany
Phone: +49-6151167066
rtrapero@cs.tu-darmstadt.de

Abstract – Pervasive computing requires a proper identity management approach so technology can actually become invisible to the user, realizing Weiser's original vision of *"the Computer for the Twenty-First Century*". We argue that identity must be understood and implemented by efficiently blending the physical and online layers where users, devices and services are present. The concept of dynamic Federated Identity Management (FIM) is the key to achieve such level of identity blending and natural integration, and it has indeed been identified as having the potential to revolutionize the Internet marketplace. The contributions of this paper include: 1) the definition of *Blended Identity* as the driving principle for applying FIM in open environments like Pervasive Computing; 2) an architectural framework for its implementation; and 3) the design and evaluation of the risk assessment methodology, the main pillar of the proposed architecture.

Keywords – Security, Identity Management, Pervasive Computing, Blended Identity, Risk Assessment

Introduction

The adoption of every new computing paradigm has been usually hindered by the security challenges it brings. In the specific field of Pervasive Computing, there is an element of paramount importance that still requires deeper research: Identity Management (IdM). In fact, Weiser's [1] vision of a world where technology becomes invisible to support people in their everyday live is currently unrealizable without a continuous authentication system.

In a ubiquitous world, a change of context (e.g., user enters a different location or new people appear in the proximity) may involve new devices, services and possibilities of interaction. It is important to note that in order for a user to gain access to pervasive services she should authenticate and expose different forms of her identity, which indeed worsen user experience and conflict with the goal of invisibility.

Identity management technologies have evolved to cope with the increasing number of services a user may access, and the so-called Federated IdM or FIM paradigm is the latest approach. The ultimate goal of FIM is to enable users of one domain to securely access data or systems of another domain seamlessly, being Single Sign-On (SSO) the most popular functionality. However, current federation technologies rely on pre-configured static agreements, which are not well suited for open environments like Pervasive Computing scenarios. These limitations have a negative impact on scalability and flexibility.

We argue that a new identity model for open environments should be defined. Thus, our contribution includes:

- The definition of the Blended Identity concept, which sets the basis for applying FIM in open environments
- A prototype of a risk-based architecture that extends and improves FIM to allow the creation of dynamic federations
- The design and validation of the risk assessment methodology that constitutes the main pillar of the proposed architecture

This proposal enables continuous authentication so that users are able to access services anytime anywhere in a secure way and minimizing user required interaction. The model is thus aligned with the basic goals of Pervasive Computing: invisibility, flexibility, scalability, and personalization.

The Challenge of Pervasive IdM

Background and Issues

When the first computers appeared, password-based authentication was the approach to handle identity. This mechanism worked pretty well at that time, due largely to how little data they actually needed to protect. However, with the advent of the Internet, the explosion of personal devices, online applications and the increase of transactions, identity got far more complex. Today, we are asked to prove our identities every time we board a plane, check into a hotel, make a purchase via credit card, or log onto a computer, smartphone, smart-TV, website, etc. Therefore, users face a mental burden, known as “*password fatigue”*, which frequently leads them to devise strategies that degrade the security of their protected information (e.g., “Poor Man SSO” strategy, which consists of always reusing the same passwords).

With the aim to ameliorate the problems related to password-based authentication, Federated Identity Management frameworks and protocols (i.e., SAML, WS-Federation, OAuth and OpenID) [2] came into scene in the last decade to allow identity portability across disparate domains. Successful implementations have been deployed in the web domain, especially in the educational and research field and in the social Internet arena. Though this is an advance on identity management, there are still important open issues.

There are two influential works [3][4] that analyze IdM problems and formulate “7 Laws” and “7 Flaws” of identity, respectively. Both studies point out security aspects (e.g., privacy, minimal disclosure, mutual authentication, etc) and effective human integration (e.g., natural interaction, easy interfaces, etc) are

Definitions and Scope

Pervasive Computing is an advanced concept where computing is made to appear everywhere and anywhere. The goal is to create ambient intelligence where network devices embedded in the environment (from clothing to cars to homes to the human body) provide unobtrusive connectivity and services all the time, thus improving human experience and quality of life without explicit awareness of the underlying communications and computing technologies.

Identity Management (IdM) describes the management of individual principals, their authentication, authorization, and privileges within or across system boundaries with the goal of increasing security and productivity.

Federated Identity Management (FIM) is the common set of policies, practices and protocols put in place to link a person's electronic identity and attributes, stored across multiple IdM systems.

Continuous Authentication refers to the set of mechanisms that allow a user to be authenticated continuously throughout her sessions, and not just at the beginning.

Risk Assessment is the identification, evaluation, and estimation of quantitative or qualitative risk levels related to a concrete situation, the comparison of these levels against benchmarks, and the determination of an acceptable risk level.

Building on the above concepts, this paper elaborates a technical-based definition of **Blended Identity**, which has been only approached so far from a social science perspective [8] . Blended Identity implies the merged IdM of online and physical identities in a pervasive environment. Given the broad set of functions that IdM involves, the paper is focused on a specific subset: the exchange of user authentication data. More specifically, it is centered on the problem of achieving continuous authentication, i.e., seamless SSO across all services and devices. The proposed underlying mechanisms based on risk are anyway applicable for the rest of cases without loss of generality.

indispensable requirements. Furthermore, they highlight trust establishment as key for scalability. While security aspects can be easily covered by FIM protocols, usability and trust challenges remain unsolved.

Despite the fact that the research community has already addressed IdM in Pervasive Computing, there is still scarce work in the context of applying FIM to it. Some proposals introduce mechanisms for SSO and seamless access control [5][6], but usually limited to a particular scenario or set of devices. So there is a need to evolve one step further in IdM, and the merging and usage of well-known FIM protocols seems a natural approach

Blended Identity

According to the exposed reasons, identity should be re-formulated for the application of FIM in Pervasive Computing. What the 7 (F)Laws miss to address is the notion of convergence between the physical and the online planes. This concern, added to the proper handling of human interaction and trust management leads to the concept of Blended Identity.

Identity has a digital part, as well as physical one. Some entities may have just an online or physical representation, while other entities may have a presence in both planes. The key to manage identity is not only in the relationships between these entities in the same planes, but also across them.

Users move around the pervasive world carrying a set of personal devices, which conforms a personal network (PN). This network is dynamic since it changes when moving for example from a smart home to a smart office or any other smart space. Devices join and leave, services appear and disappear, and access control must be re-adapted maintaining the user perception to be continuously and automatically authenticated. For this, federations must be established, i.e., creating trust relationships between devices and services to securely exchange identity data. For example, once the user logs in her smartphone, authentication is seamlessly transferred to the rest of devices on her PN. When she moves to the office, the authentication provided by the smartphone is not enough to access office devices, such as a printer, or a bunch of corporate web services. Thus, another identity source (the online corporate database) is required to provide the job identity of the user and extend and establish a federation with her PN, both for physical and online access. And all of this should happen in the background beyond user consciousness.

Hence, there is a number of coexisting identity sources, called Identity Providers (IdPs), and a number of services requiring identity data, which are offered by service providers (SPs). Roles can shift and services are offered by physical devices as well as by online providers. A universal IdP cannot be assumed since SPs will require different identity assurances and attributes in different contexts. Furthermore, in pervasive scenarios it is not realistic to assume that interactions always take place between known entities, or that the required trust relationships have been pre-configured by an administrator between every party in order to guarantee secure operations. Pervasive environments are dynamic, multi-provider and multi-service. Pre-configuration is not feasible, since it simply does not scale.

Current FIM protocols [2] are thus limited to provide this blending of identity between entities. Nowadays, it is only possible to achieve SSO across online services (in closed domains), and having manually established a previous trust relationship. Apart from lacking flexibility, the rest of possible relationships are neglected: SSO across devices in a PN, establishment of PN-federations with other PNs or with smart environments, SSO from physical devices to online services, and SSO from online services to physical devices.

Blended Identity embodies the explained concerns, and can be summarized by its main goal and underlying requirements:

***Goal**: Identity management for Pervasive Computing should efficiently blend the physical and digital planes. Users will be automatically and continuously authenticated to the smart services and devices, whether online or in their surroundings, and the environment will be adapted and personalized accordingly.*

***Requirement 1:** Natural interface. To achieve Blended Identity, an easy to use interface should be provided that automatically choses the best source of identity (IdP) and authenticates the user anytime-anywhere when changing contexts in a continuous fashion.*

***Requirement 2:** Dynamic trust relationships. To achieve Blended Identity, relationships between SPs and IdPs should not be only based on pre-configuration. It should be possible to establish new trust connections based on risk assessment.*

Related Work and Potential Impact

There are alternative proposals to achieve more streamlined ways of authentication in Pervasive Computing environments, yet they have their own flaws. The most salient work is Stajano's PICO [6]. The design proposed is based on a hardware token called Pico that relieves the user from having to remember passwords and PINs. Unlike other works, it addresses not only the case of web authentication, but also applies to all the other contexts in which users must remember passwords, providing continuous authentication. However, users must carry a new dedicated device; and this dedicated device only unlocks when other user devices are reachable to guarantee that it has not been stolen (but what if the user forgets one of her devices?). Furthermore, SSO is performed by using a new token-based protocol instead of leveraging existing working standards.

Another approach close to this work is the security architecture proposed in [5]. It allows SSO between user devices and services based on a set of software agents implementing token-based continuous authentication. In this case, a general purpose device acts as the center of authentication avoiding the need to carry yet another device. But, like PICO, it also does not build on standard protocols.

Other researchers have explored related concepts such as progressive authentication, or implicit authentication [7]. Progressive authentication consists on constantly collecting cues about the user to determine a level of confidence in her authenticity. Based on this confidence level and per application degree of protection, the system determines whether authentication is required or not. On the other hand, implicit authentication analyzes behavioral evidences to determine if an authenticated user is still using a device or the session should be closed. The aim of these approaches is to reduce the number of times a user is requested to authenticate to a particular device, but they do not address SSO. Thus, they can be understood as complementary to our work.

Summarizing, compared to the related work, our solution has three big advantages:

1. It does not require the user to carry yet another device.
2. It leverages current FIM protocols for SSO, which are properly integrated and extended. Thus, it is easier to deploy than other solutions defining new protocols, and it is compatible with existing providers.
3. In the case where interacting parties are unknown to each other, a new trust relationship can be established based on risk assessment, providing greater flexibility and scalability.

The proposed solution integrates different sources of authentication and identity data in a natural way. One of the most relevant aspects, which is not covered by any of the solutions in the related work, is the dynamic establishment of federations between previously unknown IdPs and SPs. This powerful feature has a potential positive impact in business ecosystems, since instant virtual enterprises (IVEs) could be created at any moment and share user data to offer personalized services. The user will be constantly authenticated across these services enjoying a real ubiquitous experience.

Prototyping a system for continuous authentication

Figure 1 shows the architecture for implementing continuous authentication. Since it is based on FIM standards, it also provides security services (i.e., authorization, integrity, and confidentiality) and enhanced services and privacy mechanisms (SSO, Single LogOut-SLO, account linkage, and transient and persistent pseudonym identifiers) [2]. Furthermore, it meets the additional requirements on interface design and dynamic trust establishment in order to realize the Blended Identity vision.

The main element of the architecture is the user **primary device**, i.e., any user's device that includes the modules, which acts as IdP or IdP-proxy. When operating as IdP, the device directly provides user identity data that does not require third party attestation (e.g., to authenticate against other devices belonging to the user). And when operating as IdP-proxy, it will select and re-route authentication requests to the most suitable IdP so continuous SSO is performed following the operation flow explained later. These requests can be processed in any of the existing FIM protocols, through the **FIM Connectors** module.

To achieve such level of intelligence and automation, the primary device stores user's IdPs and the passwords, credentials or tokens to access them (**Identity Data Layer**) in a tamper-proof place. In order to unlock this knowledge and let the device authenticate the user on her behalf, a biometric prove is given (e.g., fingerprint recognition). This mechanism constitutes a simple interface which is always the same, is natural, is easy and requires just a light user interaction. Thus, the proposed design is based on the common three-factor identity paradigm, which defines identity as being composed by "something-you-have", "something-you-are", and "something-you-know". Our prototype blends these three features to construct a natural way of interaction, where the primary device represents the "something-you-have", biometrics provide the "something you are", and the "something-you-know" (i.e., passwords) is transferred to "something-your-smart-device-knows" in order to improve usability and reduce users' mental overhead. This part of the architecture meets the first requirement for Blended Identity.

Apart from the explained natural interface, the key software module is the **Dynamic FIM Manager**, which includes the ***Trust Manager*** and the ***Risk Manager***. On the one hand, the Trust Manager is in charge of gathering external information and reputation data (details of operation can be found in [9]). On the other hand, the Risk Manager function is to compute the risk of collaborating with an unknown provider. Both trust and risk values are considered to decide whether to establish a relationship or not. This part of the architecture meets the second requirement for Blended Identity.

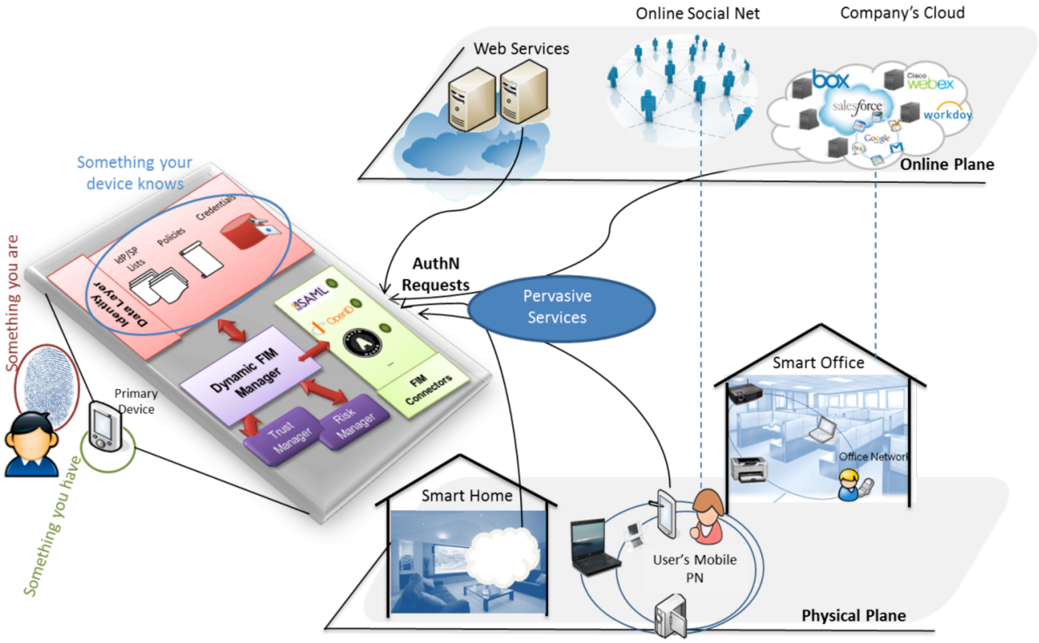


Figure 1: Architecture for Blended ID implementation

Based on the described architecture, the operation flow for continuous authentication would be the following:

1. A pervasive service offered by a SP requires user identity data (i.e., for access control), so it sends an authentication request to the user primary device
2. The user primary device executes an identity matching algorithm to determine the most suitable IdP to answer the authentication request (based on local policies) and re-routes it.
3. The selected IdP (or the device itself) decides whether to authenticate the user against the SP or not:
    a. If the SP is known and a trust relationship exists, SSO goes on by exchanging the messages of the FIM protocol in use and the user is authenticated.
    b. If the SP is unknown, the IdP gathers publicly available information about it (i.e., metadata, policies, and reputation), assesses risk, and decides *on-the-fly* whether or not federate and share identity data. The reputation protocol has been designed to avoid attacks from malicious nodes [10] as it has been also investigated in related work [11] . The reputation and risk data are combined using fuzzy logic based on [12] . The complexity of the relationship between these two factors is tackled through linguistic labels to assign quantitative values from thresholds, which allows making a decision about cooperation using conditional rules. We term this process of establishing a new trust relationship Dynamic Federation. Once completed, SSO goes on by exchanging the messages of the FIM protocol in use and the user is authenticated.
4. The authenticated user is granted seamless access to the pervasive service.

According to SSO standard protocols, an active session on the IdP is required to transparently notify the authentication state to requesting SPs, otherwise the user would be first queried to provide her credentials. This proposed architecture only requires an active session on the primary device (i.e., unlocked with fingerprint or biometric proof). Thus, the device itself will authenticate to the rest of the IdPs on behalf of the user whenever it is required by sending her credentials.

The rest of the paper is dedicated to detail the designed risk model and show its benefits and validation for pervasive IdM.

Risk assessment methodology

Deciding whether federating an SP with an IdP or not is not a trivial task. Decision-making techniques assist in this procedure, so we propose a methodology that provides a meaningful numerical model based on Multicriteria Decision Making (MCDM), which uses multidimensional risk based inputs to evaluate the suitability of the federation.

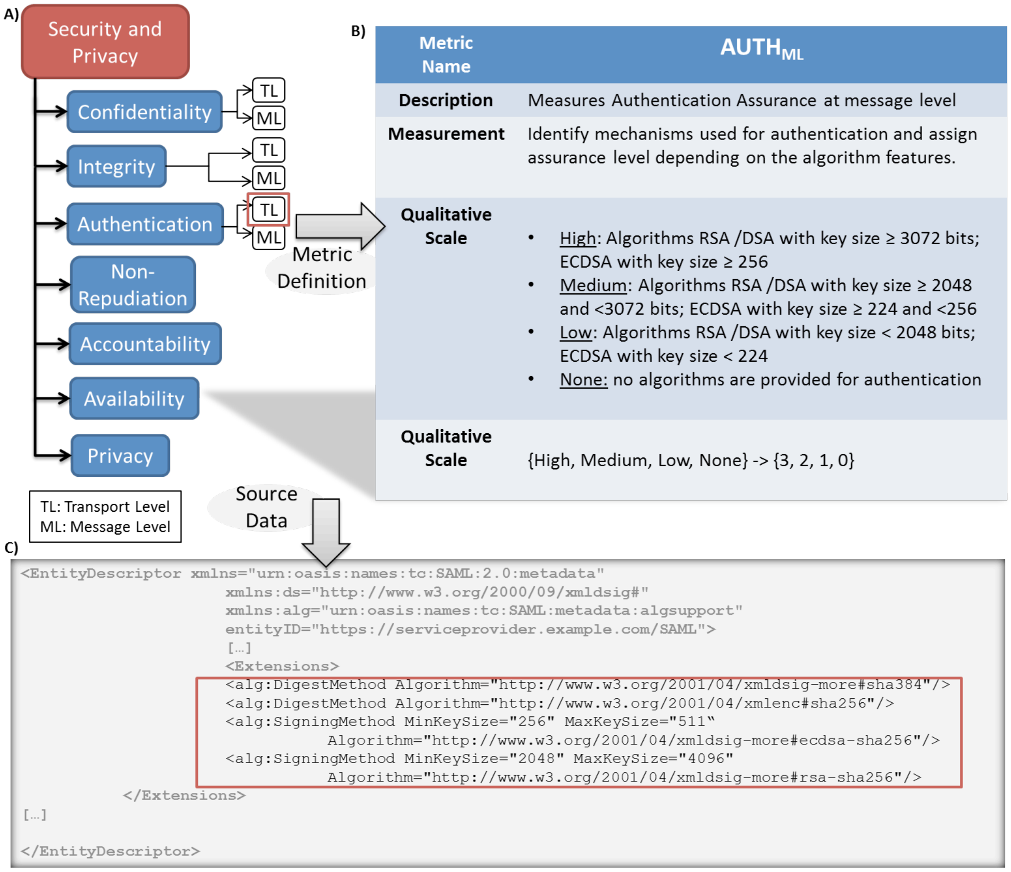
The specific technique we use is Multi Attribute Utility Theory (MAUT)[13] , which compiles: (i) the list of aspects $(N = 1, \dots , n)$ that are relevant for risk evaluation; (ii) a partial score $g_i(A)$ that indicates how good a provider A under evaluation is for each aspect according to a measurement scale $S_i \in R$; and (iii) the specific importance of each criterion under the context of the concerned provider (W_i).

The list of aspects that are considered in our risk assessment methodology are directly derived from a taxonomy tailored for FIM [14] , which was created by analyzing FIM specifications and the public survey of Research and Education Federations (REFEDS https://refeds.terena.org/index.php/Federations). The aforementioned taxonomy considers a hierarchical-based approach including two branches with five high level categories (Security and Privacy, Knowledge, Interoperability, Service Specific risks and Historical Interactions), each of them with a set of sub-criteria in the lower levels of the taxonomy.

For assigning the partial scores $g_i(A)$, we have defined a set of metrics related to every taxonomic category. In this paper we are going to focus on assurance metrics[1] (or assurance levels) that we have defined as the inverse to the probability of incurring in risk. The process of defining the applicable metrics depends on the MAUT theory, which requires numerical values between 0 and 1. However, the format of the scale used to define assurance scales is mostly qualitative, ranging from "*No assurance*", to "*Low*", "*Medium*" or "*High*". To solve this issue we map each qualitative value to a quantitative one (0, 1, 2 or 3), which is then normalized. The final result is a vector that represents the partial normalized scores for each sub-criterion $([g_1(A), \dots , g_n(A)])$ and that we term *Score Vector (SV)*.

Figure 2 exemplifies the quantification process for the metric "*Security and Privacy*", including the mapping from the qualitative scale to the quantitative scale. The bottom of the figure represents the source that is used to quantify the "*Security and Privacy*" metric that, in this example, is taken from the SAML metadata offered by a provider.

[1] During the paper we refer to the assurance metrics as risk scores since they are inversely proportional: the higher the assurance, the lesser the risk and vice versa.



Metric Name	AUTH_{ML}
Description	Measures Authentication Assurance at message level
Measurement	Identify mechanisms used for authentication and assign assurance level depending on the algorithm features.
Qualitative Scale	• <u>High</u>: Algorithms RSA /DSA with key size ≥ 3072 bits; ECDSA with key size ≥ 256 • <u>Medium</u>: Algorithms RSA /DSA with key size ≥ 2048 and <3072 bits; ECDSA with key size ≥ 224 and <256 • <u>Low</u>: Algorithms RSA /DSA with key size < 2048 bits; ECDSA with key size < 224 • <u>None:</u> no algorithms are provided for authentication
Qualitative Scale	{High, Medium, Low, None} -> {3, 2, 1, 0}

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
                      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                      xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport"
                      entityID="https://serviceprovider.example.com/SAML">
                      [...]
                      <Extensions>
                      <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha384"/>
                      <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                      <alg:SigningMethod MinKeySize="256" MaxKeySize="511"
                                 Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
                      <alg:SigningMethod MinKeySize="2048" MaxKeySize="4096"
                                 Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
           </Extensions>
[...]

</EntityDescriptor>
```

Figure 2: **A)** Part of the taxonomy that identifies Security and Privacy risk criteria. **B)** Example of metric definition related to the Authentication at Message Level (AUTH_{ML}) taxonomic dimension. Values are obtained based on the strength of the cryptographic algorithms in place, according to NIST recommendations [15] . **C)** SAML Metadata of a provider containing the information used to obtain the AUTH_{ML} metric.

The next step of the methodology consists of determining the importance of each criterion with respect to the other. For this purpose we use weights w_i that are assigned by each provider according to its own preferences and expressed in the form of a *Weight Vector* (*WV)*. With all this information we obtain the global risk score (*Agg(A)*) that is acceptable for an specific provider by aggregating all the weighted quantified criteria. Box C in Figure 3 shows this process. However, the problem is not totally solved yet.

On the one hand, given that the result obtained is a balanced combination of the criteria, meaningful differences in partial scores may lead to erroneous assessments due to compensation effects, which may indeed hide relevant information in the final value. On the other hand, there is no guarantee that minimum requirements are satisfied with this initial approach.

To solve these issues we have designed a weighing mechanism that is based on *Reference Vectors (RV)*, which contain the minimum required values for each criterion. The specific content of the *RV* will vary from one provider to another and will depend of local risk policies. Following this vector notation, box A in Figure 3 represents how to obtain the *WV* taking as input the *RV* and capturing the relative importance of each criterion. For the sake of completion we have also defined *the Assurance Compliance Index (ACI)*, which is depicted by box B in Figure 3.

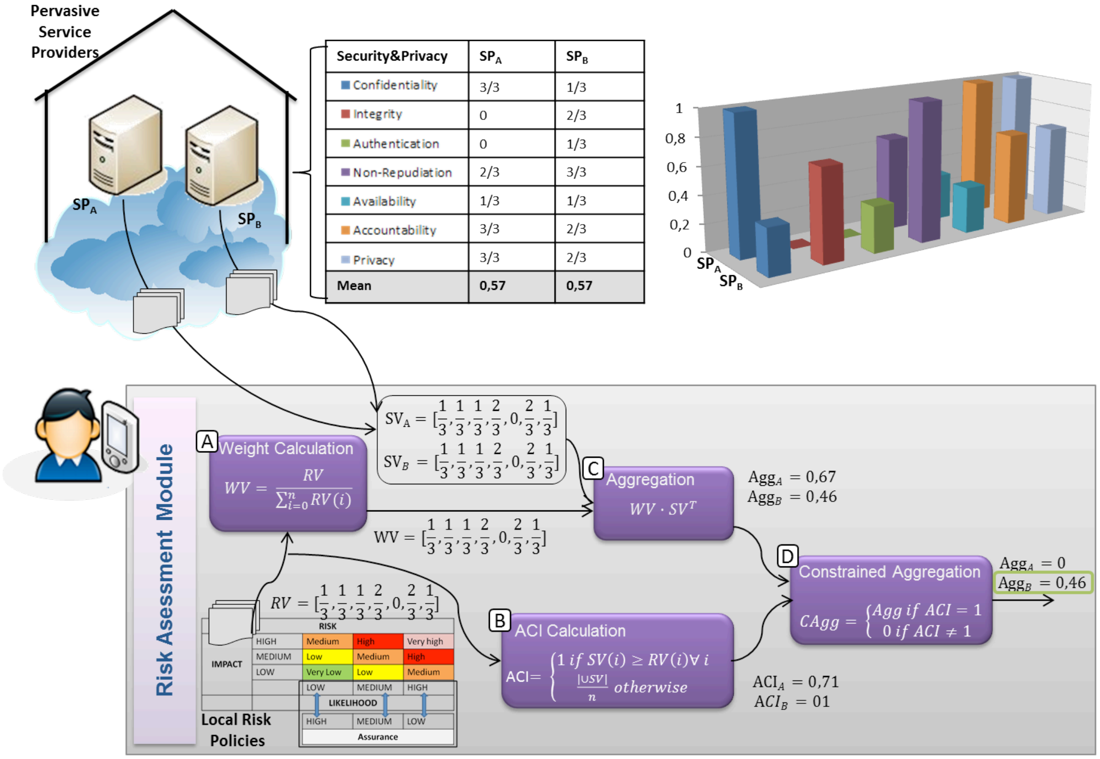
The ACI indicates the degree of compliance with the minimum requirements, being equal to 1 in case that all of them are fulfilled. Any other different value gives an idea of the degree of fulfillment of the requirements (percentage of coverage). Taking the ACI into consideration we also provide the *Constrained Aggregated* assurance value or *CAgg(A)* (box D in Figure 3), which directly discards those providers that do not cover the minimum requirements. In case the ACI is 1, then all the requirements are fulfilled and the final value obtained for the *CAgg(A)* is the global risk computed after applying the weighed summation. This final *CAgg(A)* is the value that will be considered to whether accept a dynamic federation establishment or not.

Validation

To prove the presented ideas we are following a modular approach, i.e., implementing and testing separately the different parts of the architecture in order to later integrate them in a fully working prototype. We show the validation, through a use-case, of the mathematical risk model that underlies dynamic identity federation. Moreover, we explain the implementation details.

Risk evaluation

For testing the risk model, we use SAML metadata documents available in public repositories. We have selected two providers, which we will call SP A and SP B, and inferred relevant risk-related features from their metadata. For simplicity, we just present the results for the aggregation of risk under the "Security and Privacy" category, but the rest of possible criteria would be aggregated the same way.


Pervasive Service Providers
SP_A
SP_B
1
0,8
0,6
0,4
0,2
0
SP_A
SP_B
Risk Asessment Module
A
Weight Calculation
$WV = \frac{RV}{\sum_{i=0}^{n} RV(i)}$
$SV_A = [\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},0,\frac{2}{3},\frac{1}{3}]$
$SV_B = [\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},0,\frac{2}{3},\frac{1}{3}]$
C
Aggregation
$WV \cdot SV^T$
$Agg_A = 0,67$
$Agg_B = 0,46$
$WV = [\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},0,\frac{2}{3},\frac{1}{3}]$
D
Constrained Aggregation
$CAgg = \begin{cases} Agg \; if \; ACI = 1 \\ 0 \; if \; ACI \neq 1 \end{cases}$
$Agg_A = 0$
$Agg_B = 0,46$
$RV = [\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},0,\frac{2}{3},\frac{1}{3}]$
B
ACI Calculation
$ACI = \begin{cases} 1 \; if \; SV(i) \geq RV(i) \forall i \\ \frac{|USV|}{n} \; otherwise \end{cases}$
$ACI_A = 0,71$
$ACI_B = 01$
RISK
IMPACT
HIGH
MEDIUM
LOW
Medium
High
Very high
Low
Medium
High
Very Low
Low
Medium
LOW
MEDIUM
HIGH
LIKELIHOOD
HIGH
MEDIUM
LOW
Assurance
Local Risk Policies

Security&Privacy	SP_A	SP_B
🟦 Confidentiality	3/3	1/3
🟥 Integrity	0	2/3
🟩 Authentication	0	1/3
🟪 Non-Repudiation	2/3	3/3
🟦 Availability	1/3	1/3
🟧 Accountability	3/3	2/3
🟦 Privacy	3/3	2/3
Mean	**0,57**	**0,57**

Figure 3: Risk-driven provider selection. The Risk Manager aggregates risk based on the Security and Privacy criteria for SP A and SP B, compares them and outputs a decision.

Figure 3 shows the aggregation Security and Privacy risks for SP A and B, both graphically and mathematically. Each sub-criterion is evaluated against a 4-level assurance scale ranging from 0 to 3, so for example, a value equal to 2/3 means that the third assurance level is fulfilled.

The score values for each SP are contained in the table in the upper left part of the image. Furthermore, the assurance profile graphs next to the table show how there are important differences between the values of the security dimensions for each provider.

Assuming the evaluating entity (user primary device acting as IdP) has the RV shown in the table, which leads to the associated WV, we can see that some dimensions have higher minimum assurance requirements than others. If the arithmetic mean was applied to aggregate the risk, then the two providers would have the same final security assurance value, even despite they have different profiles and despite SP A clearly does not fulfill the minimum requirements imposed by the airline. This fact is better depicted in the spider-web graph that draws the reference vector together with the score vectors of the providers.

If we apply the proposed aggregation formula with the weights obtained from the reference vector, SP B still has better assurance than SP B. Finally, we can see that only after the inclusion of the ACI, the selection of the best SP is correctly performed. Thus, from this use-case, we prove that the risk model fulfills the initial goals: it provides a meaningful unique value, which helps in automatic decision-making.

Implementation details

We have developed a *proof-of-concept* IdM infrastructure based on open source software and we work with a SAML-based SSO scenario containing users and several providers. This infrastructure has been extended to implement the logic for dynamic identity federation. This logic modifies the original SAML flow, which directly rejects requests from unknown providers, in order to allow real time evaluation and decision-making. The user primary device is being developed compliant to the SAML Profile for mobile clients in an Android smartphone. For having a richer set of IdPs, we programmed plug-ins for well-known online social providers (e.g., Facebook). Thus, the primary device acts as both IdP and IdP-Proxy, allowing users to reuse their accounts.

Conclusions and Future Lines

Pervasive computing requires a proper IdM approach so technology can actually transcend human conscious. In this sense, FIM has a big potential to achieve this goal, and it has indeed been identified as a catalyst for the next Internet marketplace revolution [16] . However, current protocols are limited due to their lack of flexibility and there is also a gap in the usability of client implementations. We argue that a better IdM can be achieved by efficiently blending the physical and online layers were users, devices and services are present through the dynamic sharing of identity data based on trust and risk assessment. If realized, it will truly lower barriers for plug and play B2B, B2C and C2C integration, leading to highly dynamic online business ecosystems where users get an improved seamless and personalized experience.

Our proposal constitutes a new step towards better IdM in pervasive environments. The contribution embodies three aspects: first we define the concept of Blended Identity and the requirements that must be met by current FIM systems to support it; second, we propose a risk-based architecture to implement this vision,; and finally we develop a quantitative risk evaluation model to be included in the implementation. So far, we have successfully evaluated the risk aggregation model and tested through implementation the feasibility of establishing federations based on one risk dimension, though we plan to implement the whole model including all the risk criteria. Also we aim to conduct usability studies that involve real users, and performance tests for measuring overhead.

Acknowledgements

We want to thank the support of anonymous reviewers for their help to improve this manuscript.

This work was supported in part by the State of Madrid (Spain) under the contract number S2009/TIC-1650 (e-Madrid), and the Spanish Ministry of Science and Innovation under the project CONSEQUENCE (TEC2010-20572-C02-01).

References

[1] Weiser, M. (1991). “The computer for the 21st century”. *Scientific American*, 265(3), 94-104.

[2] Maler, E. and Reed, D. (2008). “The Venn of Identity: Options and Issues in Federated Identity Management”. *IEEE Security & Privacy*, 6(2):16–23.

[3] Dhamija, R., and Dusseault, L. (2008). “The seven flaws of identity management: Usability and security challenges”. *IEEE Security & Privacy*, 6(2):24-29.

[4] Cameron, K. (2005). “The laws of identity”; http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[5] Soriano, E., Ballesteros, F. J., and Guardiola, G. (2007). “Shad: a human-centered security architecture for the plan b operating system”. *Proc. 5thIEEE International Conference on Pervasive Computing and Communications*, pp. 272-282

[6] Stajano, F. (2011). “Pico: No more passwords!”. *Proc. Security Protocols Workshop*.

[7] Riva, O., Qin, C., Strauss, K., and Lymberopoulos, D. (2012). “Progressive authentication: deciding when to authenticate on mobile phones”. *Proc. 21st USENIX Security Symposium*.

[8] Baker, A.J. (2009). "Mick or Keith: blended identity of online rock fans", *Identity in the Information Society,* 2 (1):7–21.

[9] Almenárez, F., Arias, P., Díaz-Sánchez, D., Marín, S., and Sánchez, R. (2011). "fedTV: Personal Networks Federation for IdM in mobile DTV." *IEEE Transactions on Consumer Electronics,* 57(2): 499-506.

[10] Almenárez, F., Marín, A., Díaz, D., Cortés, A., Campo, C., García-Rubio, C. (2011). “Trust management for multimedia P2P applications in autonomic networking”, Ad Hoc Networks, 9(4):687-697.

[11] Sun, Y., Han, Z., Liu, K.J.R. (2008) "Defense of trust management vulnerabilities in distributed networks," *Communications Magazine, IEEE* , 46(2):112-119.

[12] Manchala, D.W. (2000). “E-commerce trust metrics and models”. IEEE Internet Computing, 4(2):36–44.

[13] Keeney, R.L. and Raiffa, H. (1993). “Decisions with multiple objectives: preferences and value trade-offs”. Cambridge University Press.

[14] Arias, P., Almenárez-Mendoza, F., Marín-López, A., Díaz-Sánchez, D., and Sánchez-Guerrero, R. (2012). “A metric-based approach to assess risk for “On Cloud” Federated Identity Management”. *Springer’s Journal of Network and Systems Management*, 20(4):513 –533.

[15] Polk, T., McKay, K., and Chokhani, S. (2014). “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations”,- NIST Special Publication 800-52, Revision 1.

[16] ETSI (2011). “Identity and access management for Networks and Services; Dynamic federation negotiation and trust management in IdM systems”.

Biographies

Patricia Arias-Cabarcos is a Researcher at the University Carlos III of Madrid (UC3M), where she obtained a PhD in Telematics Engineering. Her interests include identity management, trust models and risk assessment.

Florina Almenárez is an Associate Professor at UC3M, where she obtained a PhD in Telematics Engineering. Her research interests include trust and reputation management models, identity management and security architectures in ubiquitous computing.

Rubén Trapero is a Postdoctoral Researcher at Technische Universität Darmstadt. He has a PhD in Telecommunication Engineering from Universidad Politécnica of Madrid (UPM). His research interests include privacy, identity management and service engineering.

Daniel Díaz-Sánchez is an Associate Professor at UC3M, where he obtained a PhD in Telematics Engineering. His research interests include distributed authentication, authorization and content protection.

Andrés Marín is an Associate Professor at UC3M and holds a PhD in Telecommunication Engineering from UPM. His research interests include ubiquitous computing: limited devices, trust and security in NGN.