E-government digital identity secure infrastructure; Saudi Arabia as a case study

Written by:
Mohammad Alkahtani
Student ID:
431910629
Email:
m.alkahtani@ise.sa

Submitted to the department of Computer Science in partial fulfillment of the requirements for the course:

Course Name:	Computer Security
Course Code:	CSC 519
Course Professor:	Dr. Jalal Al-Muhtadi, jalal@ccis.edu.sa

Abstract:

This article will highlight the main topics of digital identity then it will dive into the infrastructure of digital identity in the e-government and how to secure this kind of environment. Saudi Arabia is taking as a case study for suggestion the best solution that is suite its environment and culture. Finally, it will conclude that for Saudi Arabia the best way of authentication should be managed by the Ministry Of Interior in the conclusion section.

Introduction:

To define digital identity we have to agree on a proper definition for the identity. In the footnote of [12] identity has been defined as "name, address or date of birth, or such other aspects of a person's identity as may be prescribed by the regulations for the purposes of this definition". The digital identity will be any use of digital form such as RF cards, username and password in the cyberspace to give the aspects defined in identity definition.

There are many advantages and disadvantages related to applying digital identity. One of the advantages is the ease of use; for instance a bank customer can do transactions while he/she is at home. Another advantage is that digital identity satisfies the legal requirement of identifying a person since it has been used in e-government. However, as any technology the disadvantages will not be limited to what we going to cover. The first disadvantage is that identity theft for example a hacker can false the unsecure system and become another person to that system. Second disadvantage is that the cost related to implement digital identity and securing it. Last disadvantage is that we can't assure that the authenticated identity was not authenticated under intimidation.

Infrastructure:

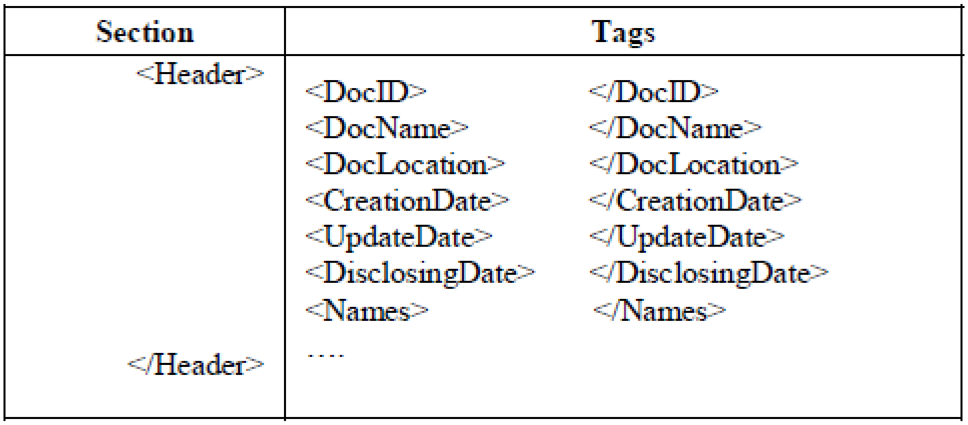
In Kingdom of Saudi Arabia all the citizens' identity role and procedure take place in Department of civil affairs belong to Ministry of Interior. However, all of the government-to-business or government-to-government transactions belong to a program called Yesser. For example if rent car officer want to assign a car to my name; so all the traffic e-ticket issued to my ID. The car rental must be subscribed with Yesser program. Yesser has a framework YEFI which standardize the data format and uses XML [14].

It is suggested that for increasing security the authentication of the citizen authenticated through ministry of interior then get the services from different businesses. For instance, if we take the car rental officer example, the office would slide the ID card which (RF Card) then the citizen enter the pin code and the authentication process authenticate through the information center of ministry of interior then both authentication the citizen and the business (car rental) passed to Yesser to give the data that the car rental authorized to see.

What is the difference between example 1 and 2? Here the car rental office will not be allowed to assign a car to a citizen without his approval (password for his digital identity).

All these process use XML and protocol such as SOAP. In [3] a Meta data for digital identity; so parties can exchange data with reduced risk. The author explains that he used Meta data because it is easy to produce because XML in each computer and digital identity document will be organized, visible and accessible. He divides the Meta data to Header which responsible of the digital identity file information as in Table 1

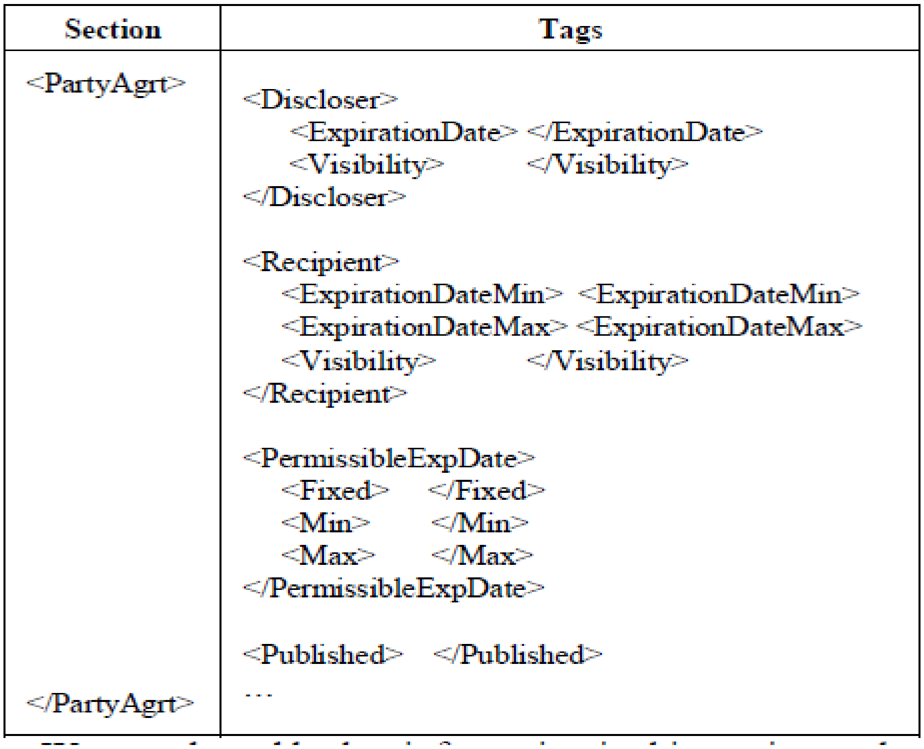
TABLE I. METADATA HEADER SECTION



Section	Tags	
<Header>	<DocID>	</DocID>
	<DocName>	</DocName>
	<DocLocation>	</DocLocation>
	<CreationDate>	</CreationDate>
	<UpdateDate>	</UpdateDate>
	<DisclosingDate>	</DisclosingDate>
	<Names>	</Names>
</Header>	….	

And a parties' agreement section which deals with roles, policies and restrictions. Table 2 shows the parties' agreement section.

TABLE II. METADATA PARTIES' AGREEMENT SECTION



Section	Tags	
<PartyAgrt>	<Discloser>	
	<ExpirationDate>	</ExpirationDate>
	<Visibility>	</Visibility>
	</Discloser>	
	<Recipient>	
	<ExpirationDateMin>	<ExpirationDateMin>
	<ExpirationDateMax>	<ExpirationDateMax>
	<Visibility>	</Visibility>
	</Recipient>	
	<PermissibleExpDate>	
	<Fixed>	</Fixed>
	<Min>	</Min>
	<Max>	</Max>
	</PermissibleExpDate>	
	<Published>	</Published>
</PartyAgrt>	…	

In our car rental example this agreement can be used with the authorization process to the citizen data.

Back to the authentication process, I will explain why it should be the ministry of interior role. First each citizen associated with unique identification number. In the citizen affairs department when and identification card issued each citizen has to enter his own password which 4 digits. The authentication process starts with a session between the citizen and the information center of ministry of interior. Session Hijack is one possible risk to identity theft. To eliminate this risk SSL must be used with certificates in both ends [6]. The certificate issuer in Saudi Arabia is National Center for Digital Certification for government and businesses. This will lead to public/private key encryption with high security measure.

In this way of authentication we are pretty sure that the authentication secure and there will be no session hijacking.

However, we have to provide the service through Yesser; so there must be a token from ministry of interior to Yesser telling Yesser to serve the request from the business (Car rental) with the citizen data. This token should use symmetric key encryption and it should be changed regularly to ensure the best practice of security and the token might the identification number of the citizen encrypted by the secret key. In this way Yesser will ignore any request that does not know the secret key. The best fit communication method is that the business sends the information to the information center of ministry of interior then wait for the replay. The information center of ministry of interior sends back the encrypted identification number of the citizen then the business starts new session with Yesser and sends the encrypted data with its username and password to Yesser. Yesser maps the citizen data to the access data limits and serve the business.

To ensure high security ministry of interior has to have access list for all the machines that will use its authentication service and ignores and request beyond this list. There must be a secure network communication between the business, ministry of interior and Yesser. This will let Yesser and ministry of interior use firewalls and core switch.

Is that enough, according to [4] and [5] a multifactor authentication must be present to ensure a secure identity and for commercial use Kingdom of Saudi Arabia has regulated the use of authentication to a digital identity to at least two factors; so most of the banks use one time authentication code sent to the customer mobile or token. The authentication for e-government I believe must use the same standard.

New Idea for authentication:

In [11] the author state that the Defense Advanced Research Projects Agency doing research for identify the person from different pattern such as the way of typing letters on the keyboard and there will be no need for password; you type only your username. This will help a lot of people who forget there password frequently.

Conclusion:

A case study has been presented for e-government digital identity for Kingdom of Saudi Arabia. It shows a complex communication and process but it ensures high security for both the government and the citizen. A research idea for new authentication procedure has sighted.

References:

[1] Agbinya, J. I., Islam, R., & Kwok, C. (2008). Development of digital environment identity (DEITY) system for online access. *2008 Third International Conference on Broadband Communications, Information Technology & Biomedical Applications*. doi: 10.1109/broadcom.2008.52

[2] Ayed, G. B., & Ghernaouti-Helie, S. (2011). Digital Identity Management within Networked Information Systems: From Vertical Silos View into Horizontal User-supremacy Processes Management. *Proceedings of the 2011 14th International Conference on Network-Based Information Systems (NBiS 2011)*. doi: 10.1109/NBiS.2011.24

[3] Ben Ayed, G. (2011). Digital identity metadata scheme: A technical approach to reduce digital identity risks. *Proceedings 2011 25th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA 2011)*. doi: 10.1109/waina.2011.118

[4] Bhargav-Spantzel, A.; Squicciarini, A.C.; Rui Xue; Bertino, E.; , "Multifactor Identity Verification Using Aggregated Proof of Knowledge," Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on , vol.40, no.4, pp.372-383, July 2010
doi: 10.1109/TSMCC.2010.2045755

[5] Camp, L. J. (2004). Digital identity. *Ieee Technology and Society Magazine, 23*(3), 34-41. doi: 10.1109/mtas.2004.1337889

[6] Choi, D., Roh, J., Kim, S., Jin, S., & Etri. (2009). *Identity Data Security System for the Digital Identity Wallet*.

[7] Corradini, F., Paganelli, E., Polzonetti, A., Forastieri, L., & Settimi, D. (2006). Smart card distribution for e-government digital identity promotion: problems and solutions. *ITI 2006 Proceedings of the 28th International Conference on Information Technology Interfaces*.

[8] Harn, L., & Ren, J. (2008). Efficient identity-based RSA multisignatures. *Computers; Security, 27*(1–2), 12-15. doi: 10.1016/j.cose.2008.03.003

[9] Jianming, Y. (2007). Digital identity design and privacy preservation for e-learning. *Proceedings of the 2007 11th International Conference on Computer Supported Cooperative Work in Design*.

[10] Jianming, Y., Tiwari, S., Xiaodi, H., & Qun, J. (2011). Constructing robust digital identity infrastructure for future networked society. *Proceedings of the 2011 15th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. doi: 10.1109/cscwd.2011.5960129

[11] STROSS, R. (2012, 17/3/2012). Bypassing the Password, Technical, *The New York Times*. Retrieved from http://www.nytimes.com/2012/03/18/business/seeking-ways-to-make-computer-passwords-unnecessary.html

[12] Sullivan, C. (2009). Digital identity – The legal person? *Computer Law; Security Review, 25*(3), 227-236. doi: 10.1016/j.clsr.2009.03.009

[13] Thorpe, S. (2010). A case analysis of a contextual model of trust for digital identities using UML 2.0 and context graph algorithms. *2010 Sixth International Conference on Information Assurance and Security (IAS 2010)*. doi: 10.1109/isias.2010.5604184

[14] YESSER. 2012. *YEFI* [Online]. Yesser. Available: http://www.yesser.gov.sa/ar/BuildingBlocks/Pages/interoperability_framework.aspx [Accessed 22/5/2012 2012].

[15] Yong, J. (2009, 14-16 Aug. 2009). *Digital identity control mechanism for e-learning.* Paper presented at the IT in Medicine & Education, 2009. ITIME '09. IEEE International Symposium on.