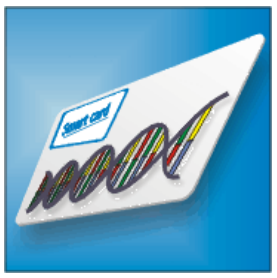
Crossroads
The ACM Student Magazine



DNA Smart Card for Financial Transactions

by ***Sofia Gleni*** and ***Panagiotis Petratos***

Introduction

In this paper, a secure environment for electronic commerce is introduced. The environment is formed via a synthesis of biometrics consumer authentication with a security token. Such a token is a smart card containing cryptographic keys and a cryptographic microprocessor for data encryption. The keys are used to further authenticate the possessor of the card as the actual owner and also to facilitate secure electronic financial transactions. New technologies like these bring benefits to society by enhancing the standard of living, however, numerous challenges are introduced [**1**].

Biometrics is a Greek composite word stemming from the synthesis of bio and metric, meaning life measurement. In this context, the science of biometrics is concerned with the accurate measurement of unique biological characteristics of an individual in order to securely identify them to a computer or other electronic system. Biological characteristics measured usually include fingerprints, voice patterns, retinal and iris scans, face patterns, and even the chemical composition of an individual's DNA [**9**].

Biometrics and Financial Transactions

Two words with essential meaning for our discussion are genotype and phenotype. **Genotype** means a genetic constitution or a group sharing it. **Phenotype** means the

actual expression of a feature through the interaction of genotype, human development, and the influence of the environment. The heritable features that are genetically determined, such as blood group and DNA sequence, are called genotypic features. The features that are further developed beyond the genetic information, such as fingerprints or iris sequences, are called phenotypic or **epigenetic** features [3, 4].

Phenotypic features also vary depending on their rate of change over time. For instance, fingerprints and facial appearance change over time, while iris texture remains unchanged for time periods spanning decades [5, 6]. Fingerprints are phenotypic features that have been used reliably as a biometric method of identification, but they do have some disadvantages. Fingerprints are subject to changes imposed by the external environment — with or without the individual's will. For example, a laborer after a few years of hard work in the fields may have fingerprints that are so faint that they are hardly identifiable. Another example pertains to criminals that have been known to dip their finger tips in acid in order to erase their fingerprints and escape prosecution.

On the other hand, an iris is isolated and protected from the external environment. The iris is an internal organ of the eye that is located behind the cornea and the aqueous humor [6]. If contemporary surgical iris modifications are attempted by unscrupulous individuals, they are subject to permanent vision damage. Finally, a natural test against deceit is the physiological iris response to light [5].

Security is not achieved by focusing on a single parameter, or solving a one-dimensional problem [8]. A secure environment requires multiple dimensions of critical check points. Having more check points in place will likely lead to a lower probability that an imposter will cross the barriers [10]. In that respect, increasing the authentication checkpoints by including both a genetic and an epigenetic feature is a more reliable and secure strategy than relying on a single feature.

This strategy can be applied to security tokens as well. Instead of using a simple magnetic stripe card with only the challenge of a personal identification number (PIN) to access a bank account, a safer approach would be to authenticate the card possessor with biometrics sensors. Biometrics authentication subsequently enables a secure token, such as a smart card. The smart card contains a cryptographic microprocessor for data encryption and cryptographic keys that further verify the card owner's identity and facilitate secure electronic commerce. For instance, the Public Key

Infrastructure (PKI), in conjunction with smart cards and biometrics authentication, can provide the necessary conditions for a secure environment.

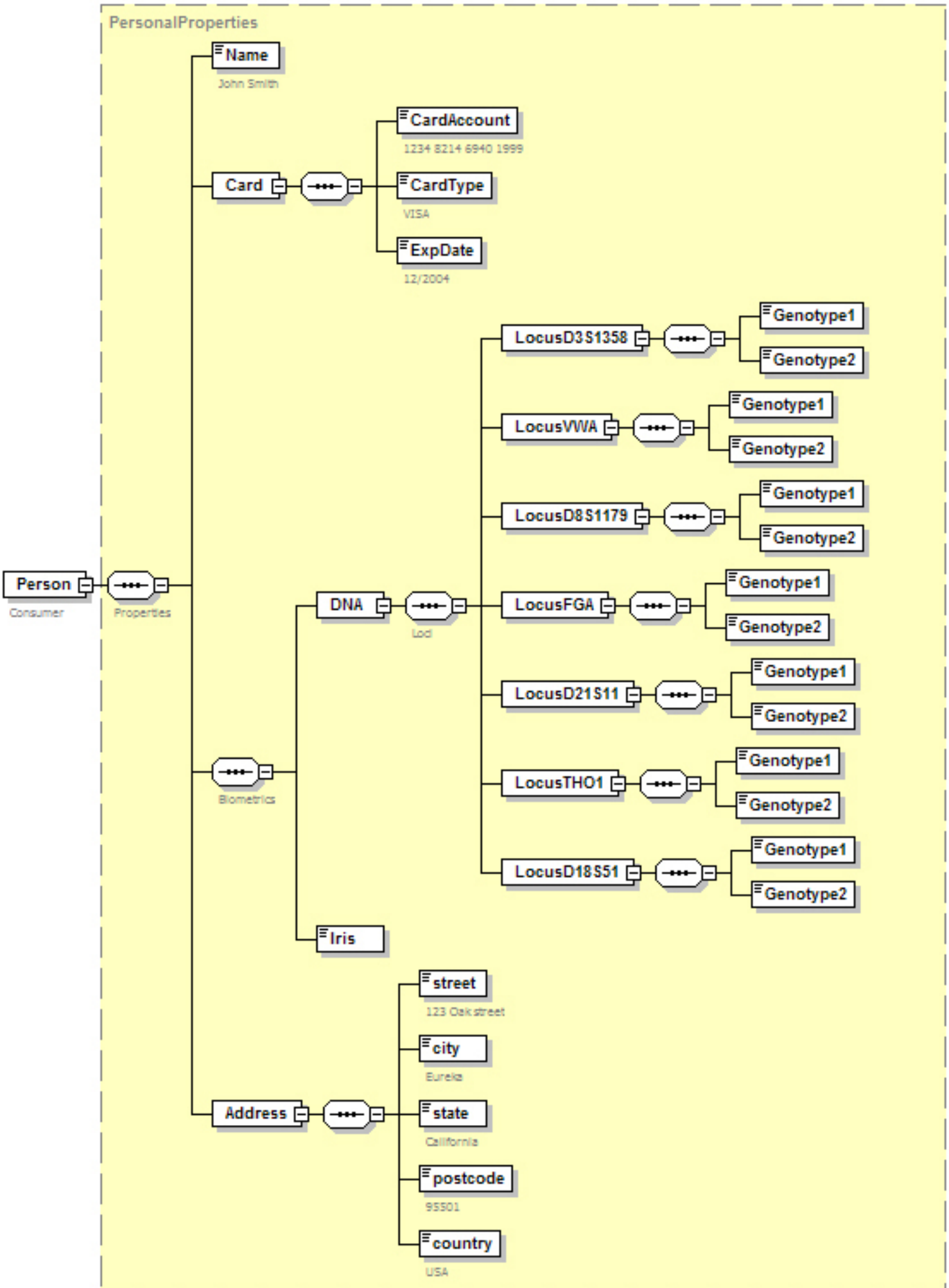
In such an environment, every user is issued two cryptographic keys: a secret private key and a public key. The public key is certified by a trusted party, such as a notary or a passport office, and is widely known. The private key remains a securely guarded secret by the owner. In this case, the secret private key is a fragment of the owner's DNA, consisting of only the genetic loci sequences necessary for identification. The cryptographic keys must be stored with a secure method. A smart card is a credit card-sized true computing device containing a microprocessor, input and output channels, and static and dynamic memory. The microprocessor is capable of a wide variety of cryptographic functions, including random number generation, digital signing, and key generation. The private key never needs to be revealed or offloaded.

A typical authentication procedure in such an environment is:

1. Insert the smart card into the card reader terminal. Cryptographic keys and iris code reside in the smart card.
2. Enter the PIN in order to enable the smart card.
3. Biometrics sensors scan the iris of the user. Comparison of the scanned iris code versus the smart card resident iris code takes place.
4. The card reader terminal generates a random number and sends it to the smart card with a request for encryption.
5. The smart card microprocessor encrypts the random number and sends it back to the card reader terminal.
6. The card reader terminal obtains the public key and decrypts the original random number. The user and card are authenticated.

Through this process, the possessor of the smart card is securely authenticated as the owner of the cryptographic keys. In order to express the owner's smart card data so that the information is available through a computer network and so that it can facilitate automatic ecommerce, the data has to be in an integrated, compatible, homogeneous, and uniform format. The XML model below (**Figure 1**) illustrates this format.

```
<?xml version="1.0" encoding="UTF-8"?>
<Person xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="C:\DNAsmartCard.xsd">
	<Name>John Smith</Name>
	<Card>
		<CardAccount>1234821469401999</CardAccount>
		<CardType>Visa</CardType>
		<ExpDate>2004-12-14</ExpDate>
	</Card>
	<DNA>
		<LocusD3S1358>
			<Genotype1>15</Genotype1>
			<Genotype2>18</Genotype2>
		</LocusD3S1358>
		<LocusVWA>
			<Genotype1>16</Genotype1>
			<Genotype2>16</Genotype2>
		</LocusVWA>
		<LocusD8S1179>
			<Genotype1>12</Genotype1>
			<Genotype2>14</Genotype2>
		</LocusD8S1179>
		<LocusFGA>
			<Genotype1>19</Genotype1>
			<Genotype2>24</Genotype2>
		</LocusFGA>
		<LocusD21S11>
			<Genotype1>29</Genotype1>
			<Genotype2>31</Genotype2>
		</LocusD21S11>
		<LocusTHO1>
			<Genotype1>8.98</Genotype1>
			<Genotype2>9.66</Genotype2>
		</LocusTHO1>
		<LocusD18S51>
			<Genotype1>12</Genotype1>
			<Genotype2>14</Genotype2>
		</LocusD18S51>
	</DNA>
	<Iris>ABBAA9FD44B12CA9CD64E12CCAFE</Iris>
	<Address>
		<street>123 Oak street</street>
		<city>Eureka</city>
		<state>California</state>
		<postcode>95501</postcode>
		<country>USA</country>
	</Address>
</Person>
```


PersonalProperties
Name
John Smith
CardAccount
1234 8214 6940 1999
Card
CardType
VISA
ExpDate
12/2004
Person
Consumer
Properties
DNA
Loci
LocusD3S1358
Genotype1
Genotype2
LocusVWA
Genotype1
Genotype2
LocusD8S1179
Genotype1
Genotype2
LocusFGA
Genotype1
Genotype2
LocusD21S11
Genotype1
Genotype2
LocusTHO1
Genotype1
Genotype2
LocusD18S51
Genotype1
Genotype2
Biometrics
Iris
street
123 Oak street
city
Eureka
Address
state
California
postcode
95501
country
USA

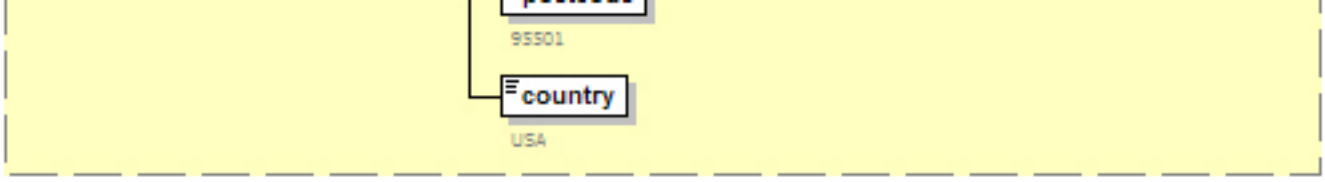


Figure 1: Example XML document and schema of the smart card data.

A large part of the human DNA sequence is identical for all individuals. Over 99% of the human genome, which is a sequence of over three billion genetic elements, is common to everyone [7]. However, there are distinguishing inherited regions of the DNA that are different from individual to individual and that constitute our genetic uniqueness. These dissimilarities in the DNA sequence are called polymorphisms and are very useful for DNA analysis and forensic identification. One class of such DNA polymorphisms is known as the Short Tandem Repeats (STRs), which are short sequences of DNA normally two to five base pairs long, repeated numerous times as head-tail lists. For instance, "gatagatagatagata" is a sixteen element, base pair sequence of four head-tail list copies of the tetramer "gata."

The different numbers of copies of the repeat list that can occur from individual to individual constitute the STRs polymorphisms. Thirteen core STR genetic loci plus one determining the gender is the current standard for the US national DNA database, also known as Combined DNA Index System (CODIS) [2]. In the example XML schema (**Figure 2**), the iris code is a single binary number while the DNA is a sequence of genetic loci each containing a pair of genotypes. Naturally the iris code and the private DNA cryptographic key are used only for authentication purposes and they are never revealed or offloaded to third parties. For instance, **Figure 2** is an example illustrating an ecommerce financial transaction for a product.

```
<?xml version="1.0" encoding="UTF-8"?>
< ipo:purchaseOrder xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="C:\ecommerce.xsd">
      <billShipTo>
            <name> John Smith </name>
            <street>123 Oak street</street>
            <city>Eureka</city>
            <state>California</state>
            <postcode>95501</postcode>
            <country>USA</country>
            <Card>
                  <CardAccount>1234821469401999</CardAccount>
                  <CardType>Visa</CardType>
                  <ExpDate>2004-12-14</ExpDate>
            </Card>
      </billShipTo>
      <Items>
            <item>
                  <productName>Hard Drive</productName>
                  <productNumber>126969</productNumber>
                  <quantity>2</quantity>
                  <price>314.69</price>
                  <comment>None</comment>
                  <shipDate>2004-04-12</shipDate>
            </item>
      </Items>
</ipo:purchaseOrder>
```

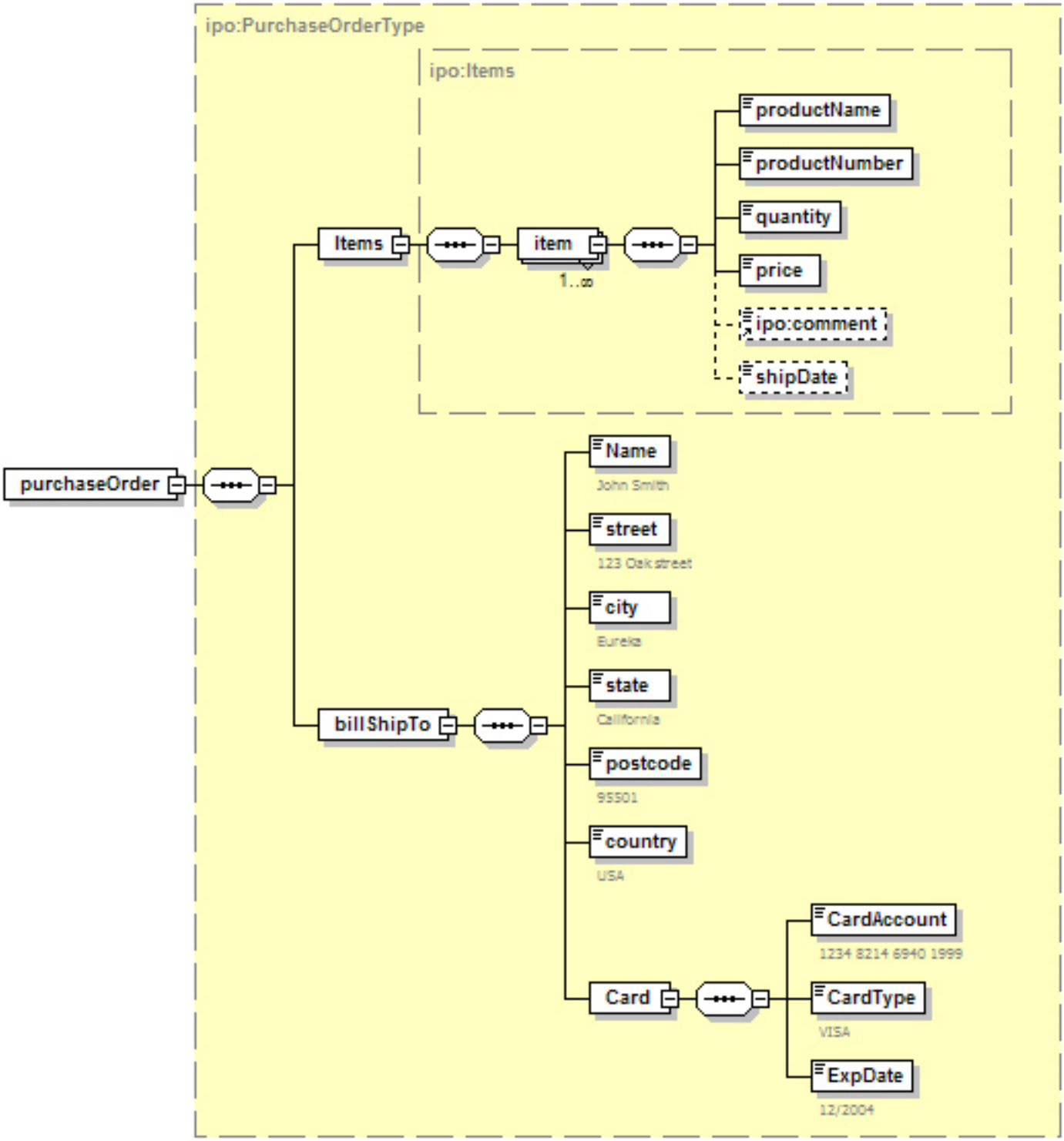


Figure 2: Example XML document and schema of a purchase order.

In contemporary financial transactions, a single PIN of a magnetic stripe card avails access. On the other hand, there is the secure environment for electronic commerce that has been introduced. In this environment biometrics authentication initially validates the card possessor. Subsequently, this procedure enables a smart card's cryptographic microprocessor, which allows bidirectional authentication through cryptographic keys. Further verification takes place between the smart card and the

card reader terminal. The environment enforces multiple layers of security and avails access to the user only through multi-dimensional authentication.

Conclusion

Security is not enforced by focusing on a single parameter. Instead of solving a one-dimensional problem, a secure environment requires multiple dimensions of critical check points. Secure authentication is provided by multiple parameters. One parameter is a security token an individual uniquely possesses, such as a physical key or a smart card. Another parameter is an item an individual uniquely knows, such as a PIN. An additional parameter is an individual's unique biological characteristic, such as DNA or an iris code. Automatic financial transactions are facilitated by this secure environment through the automated electronic verification of the identity of the consumer, which enables frictionless electronic commerce.

References

1. Alterman, A. A piece of yourself: Ethical issues in biometric identification. *Ethics and Information Technology*, December, vol. 5 num. 3, 2003.
2. Budowle, B. and Moretti, T. Genotype profiles for six population groups at the 13 CODIS short tandem repeat core loci and other PCR based loci. *Forensic Science Communications*, July, vol. 1, num. 2, 1999.
3. Daugman, J. "Phenotypic versus genotypic approaches to face recognition." In: Face Recognition: From Theory to Applications. Heidelberg: Springer-Verlag, pp. 108-123, 1998.
4. Daugman, J. Demodulation by complex-valued wavelets for stochastic pattern recognition. *International Journal of Wavelets*, Multi-resolution and Information Processing, vol. 1, num. 1, pp. 1-17, 2003.
5. Daugman, J. The importance of being random: Statistical principles of iris recognition. *Pattern Recognition*, vol. 36, num. 2, pp. 279-291, 2003.
6. Davson, H. Davson's Physiology of the Eye, 5th ed., London, Macmillan. 1990.
7. Economist Technology Quarterly, The. DNA's detective story. *The Economist*, Mar. 13, vol. 370 num. 8366, 2004.

8

Hinduja, S. Trends and patterns among online software pirates. *Ethics and Information Technology*, June, vol. 5 iss. 1, 2003.

9

IBG, International Biometric Group. Biometrics Market and Industry Report 2004-2008, IBG, New York, New York. <**http://www.biometricgroup.com**> 2004.

10

Jefferson, J. Deleting: Prosecutors Want Tough Laws to Put Internet Hackers, Scam Artists and Pedophiles on Permanent Log Off. *Cyber Law, ABA Journal*, October, 83: 68, 1997.

Biographies

Sofia Gleni (**sgleni@yahoo.co.uk**) is a postgraduate student in the Department of Computing and Information Systems at the University of Luton. Her research interests include information systems and the social, political, and economic dimensions of information and communications technology.

Panagiotis Petratos (**ppetratos@csustan.edu**) is an Assistant Professor in the Department of Computer Information Systems at CSU Stanislaus and a postgraduate student at the University of Luton. His research interests include computing and information science, information retrieval, bioinformatics, and the economic dimensions of information and communications technology.