

ID-card based authentication in public WiFi HotSpot



Imre Kuus

Sonictest Ltd.

ESTONIA

<http://www.sonictest.ee>



Introduction

- MikroTik user since 2004
- Regular european MUM visitor since 2006
- MikroTik distributor since 2007
- MikroTik trainer since 2009
- We integrate MikroTik products into customized solutions.



Project of ID card based WiFi HotSpots

- More than 100 public libraries and other places need public WiFi coverage on 2009.
- Endusers will have free WiFi and it will be provided by local municipality.
- Provided system should be capable to identify persons who are in WiFi area to follow EU directives about Internet service providing and logging sessions.



Background of the project

- ID-cards (smartcards as personal identity cards with digital signature) are in use since 15.12.2000 in Estonia.
- It is common method for authentication people in e-services provided by government institutions, banks and other companies more than 10 years now.
- Most computers have already smartcard reader and ID-card software installed.



- The ID-card is a primary personal identification document
- The ID-card can be used for using Internet-based services provided by the state as well as by several private enterprises and banks.



ID Card details

- The ID-card can be used for issuing digital signatures and identify person.
- The ID-card provides a personal @eesti.ee e-mail address
- The ID-card is the most straightforward, convenient and safe way of self defence for users of Internet banking systems and other web-based services.

ID card services

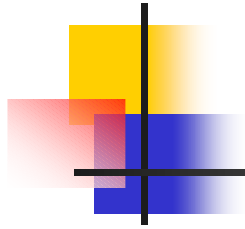
- Links to most popular e-services can be found at: <http://www.id.ee/> (also available in english)
- ID card can be used also as public transport or concert ticket and also for public Wi-Fi networks and logging into companies LAN (windows domain).





Some statistics about ID cards

- Estonia has 1 340 122 people 01.01.2011
- On the 07.03.2011 we had:
 - Active cards: 1 145 342
 - Digital signatures given: 49 108 223
 - Electronic authentications: 83 587 491



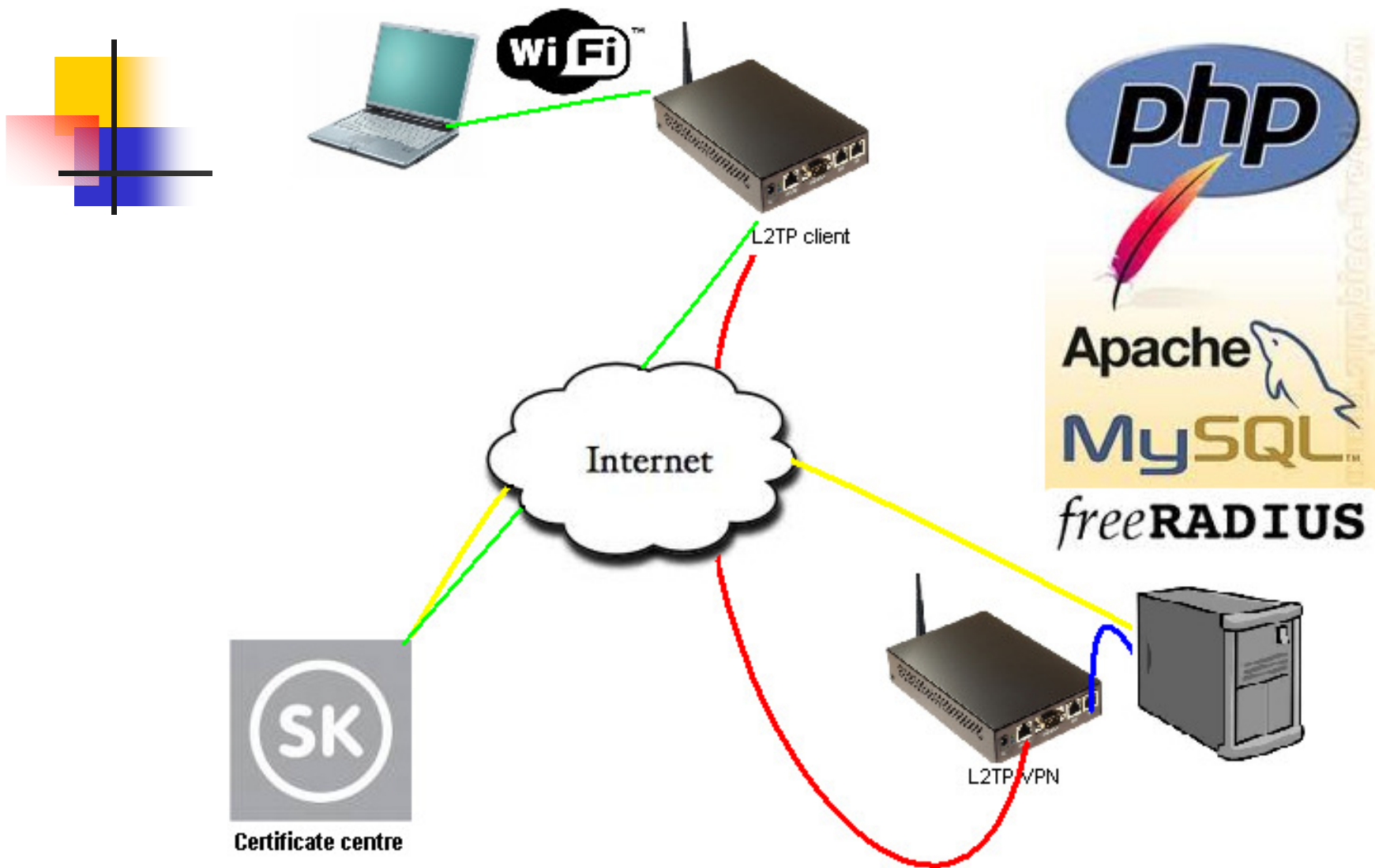
ID-card software

- ID-card software is provided by SK (Certification Centre, legal name is AS Sertifitseerimiskeskus)
- It is Estonia's primary and currently the only certification authority (CA), providing certificates for authentication and digital signing to Estonian ID Cards.
- Client software is available for:
 - Windows operating systems
 - Mac OS
 - Linux (Estobuntu distribution has it by default)

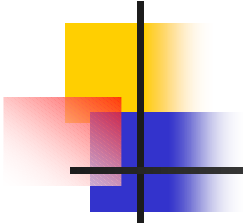


In order to use the ID-card electronically, you need the following:

- the ID-card with its PIN codes;
- A computer with operating system and browser;
- a smart card reader;
- ID-card software from <http://installer.id.ee>
- Internet connection
- Insert the card into the reader before the use of the service and leave it in the reader for the entire session time.
- You are prompted to enter your PIN codes upon the use of electronic services.

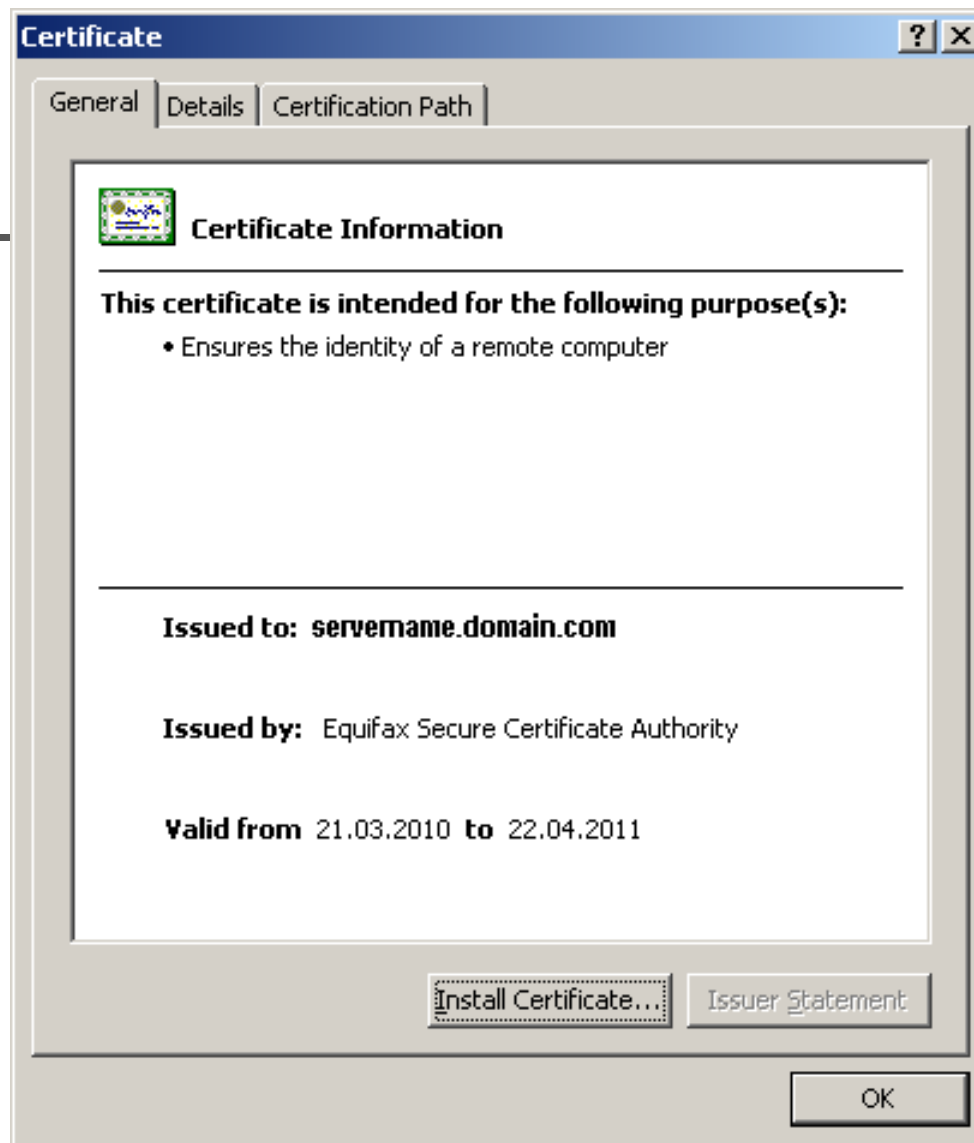
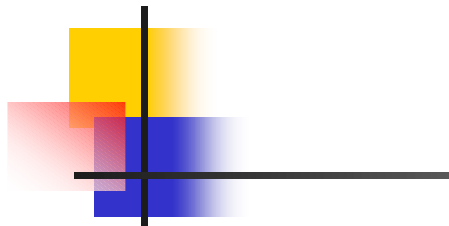


How this works?



- Quick answer is with 2 certificates and web/DB/radius server:
- **A certificate** is a proof by which one user introduces him- or herself to another (e.g., a conversation partner or a server) and makes a transaction based on this identification, by issuing a digital signature, for example.
- **A device certificate** is a proof issued by the Certification Centre to an owner of an electronic device or a server. The device or the server proves the authenticity of its identity to other persons or devices.
- A typical device certificate is a https web server certificate, by which a web server proves its "authenticity" to users.

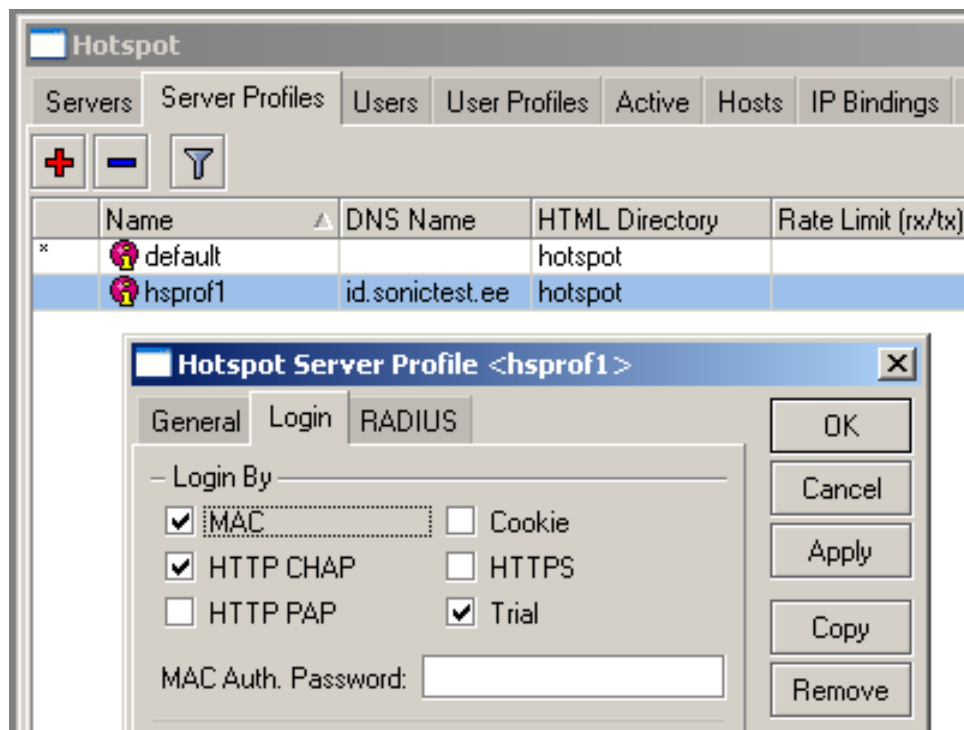






What we need to do?

- First we need to understand what customer needs and then adjust all systems to make it happen for them with keeping in mind also TCO.
- In MikroTik RouterOS most of You knew that there is no option for ID-Card authentication in MT hotspot server profile.
- But there is possible to use Radius, MAC, http-chap and trial user.
But we can use them all at the same time.





Tools required for that.

- Thanks to MikroTik people there is good possibilities for modifying HotSpot startpage to fit your needs. All you need is JavaScript, HTML knowledge and graphical design.
- Easily dublicateable advanced RouterOS configuration.
- Linux OS server with apache https webserver with SSL certificate and PHP, MySQL for database and freeradius as radiusserver



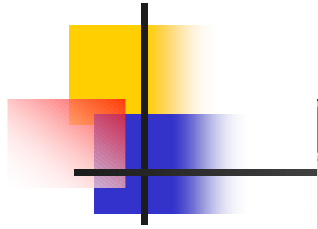
What information we need?


- According to EU directives ISP should be able to answer to police questions like: who used internet with this public IP on certain time?
- So we need to collect following data:
 - Persons name and surname, personal ID code,
 - endusers device MAC,
 - public IP of this WiFi router at that time
 - start and end time of the internet session.



Where we can get information?

- ID card contains person's ID code and name. It is possible to read this from card if user enters PIN, when asked.
- Using HotSpot startpage, we can read MAC address of the users laptop network card.
- We can get public IP addresses by saving VPN server log (PPP active connections list) to syslog server database.
- Radius server and MySQL can be used for logging users sessions start and end time.






















 7d

- Interfaces
- Wireless
- Bridge
- Mesh
- PPP
- IP
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Make Supout.tif
- Manual
- Exit

ppp

Interface PPPoE Servers Secrets Profiles Active Connections

  Find

	Name	Caller ID	Uptime	
L		88.196.78	2d 13:03:53	
L		217.159.2	2d 13:03:53	
L		217.159.2	2d 13:03:53	
L		88.196.17	2d 13:03:53	
L		213.219.9	2d 13:03:52	
L		88.196.27	2d 13:03:52	
L		90.190.10	2d 13:03:52	
L		217.159.2	2d 13:03:52	
L		80.235.50	2d 13:03:52	
L		88.196.38	2d 13:03:52	
L		90.190.52	2d 13:03:52	
L		213.35.22	2d 13:03:51	
L		88.196.17	2d 13:03:51	
L		90.191.68	2d 13:03:50	
L		88.196.52	2d 13:03:50	
L		95.153.58	2d 13:03:50	
L		62.65.35	2d 13:03:50	

66 items



What about people without ID Card?

- For avoiding situations when someone does not have ID Card and wants to use WiFi, we made it possible to use internet also with username and password, that is possible to get from local libraries.
- Library workers have web-based user interface in Radius server for making users to their WiFi HotSpot. They should identify persons with other documents like driver's license or passport and fill the form.

New user creation form.

Adminpaneel -> Avalik internet

*** EML avalik WiFi leviala => [3 RK] ***

[[Logi välja](#)] Sortimine: ▲KASUTAJA▼ ▲EESNIMI▼ ▲PEREKONNANIMI▼

[[kasutajad](#)]
Avalik internet
[[Statistika](#)]

Kasutaja: Eesnimi:
Parool: Perekonnanimi:
Isikukood: Kasutusaeg: 1 min
 Muudetud: 12:20:20 11.03.2011

Lehekülg: 1/1

	Kasutaja	Parool	Eesnimi	Perekonnanimi	
<input type="button" value="Uus"/>	mum	*****	MUM	Testuser	+
edit / del					
			Kokku:	1	



Lets see how it works!

- For live demo I have RB433UAH with all nessesary configuration ready.
- For the project it was nessesary to provide ready configured devices that will be sent by post to libraries and non-skilled persons will just connect the cables and it should start working at once.
- We provided also quick installation guide for doing it.

Reports if needed.

Adminpaneel -> Statistika - Windows Internet Explorer

https://servername/radiusadmin/radkasutus/?sort=AcctStartTime&order=desc&otsisona=&pa

File Edit View Favorites Tools Help

Adminpaneel -> Statistika

*** EML avalik WiFi leviala => [48 RK] ***

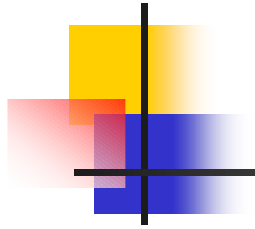
[Logi välja] Sortimine: ▲KASUTAJA▼ ▲ALGUSAEG▼

Lehekülg: 24/122

[kasutajad]
[grupid]
[õigused]
[parameetrid]
[tabelid]
[radius]
[Avalik internet]
Statistika

	Kasutajanimi	Algusaeg	Kestvus	Lõppaeg	Põhjus
576	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-11 23:31:30 3433 s	2010-07-12 00:28:43	Lost-Service
577	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-11 22:17:59 3600 s	2010-07-11 23:17:59	Session-Tim
578	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-11 21:23:14 2918 s	2010-07-11 22:11:52	Lost-Service
579	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-11 20:14:22 3600 s	2010-07-11 21:14:22	Session-Tim
580	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-11 19:12:13 3600 s	2010-07-11 20:12:13	Session-Tim
581	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-11 18:12:03 3203 s	2010-07-11 19:05:26	Lost-Service
582	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-11 14:56:27 3600 s	2010-07-11 15:56:27	Session-Tim
583	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-11 13:53:28 3600 s	2010-07-11 14:53:28	Session-Tim
584	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-11 11:36:03 3600 s	2010-07-11 12:36:03	Session-Tim
585	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-11 00:00:59 2869 s	2010-07-11 00:48:48	Lost-Service
586	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-10 22:57:36 3600 s	2010-07-10 23:57:36	Session-Tim
587	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-10 18:37:41 3600 s	2010-07-10 19:37:42	Session-Tim
588	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-10 16:48:53 3600 s	2010-07-10 17:48:53	Session-Tim
589	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-10 10:44:40 671 s	2010-07-10 10:55:51	Lost-Service
590	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-10 06:10:43 1901 s	2010-07-10 06:42:24	Lost-Service
591	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-09 23:21:42 3600 s	2010-07-10 00:21:42	Session-Tim
592	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-09 22:19:31 3600 s	2010-07-09 23:19:31	Session-Tim
593	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-09 21:19:28 3600 s	2010-07-09 22:19:28	Session-Tim
594	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-09 20:18:00 3600 s	2010-07-09 21:18:00	Session-Tim
595	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-09 00:10:47 994 s	2010-07-09 00:27:21	Lost-Service
596	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-08 22:16:54 3600 s	2010-07-08 23:16:54	Session-Tim
597	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-08 21:15:16 3600 s	2010-07-08 22:15:16	Session-Tim
598	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-08 20:13:51 3600 s	2010-07-08 21:13:51	Session-Tim
599	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-08 19:12:28 3600 s	2010-07-08 20:12:28	Session-Tim
600	RAIVO	36503111...; 00:26:5A:EE:B8:35; ...5.50.246 (ID-kaart)	2010-07-08 18:10:33 3600 s	2010-07-08 19:10:33	Session-Tim
			Kokku:	3028	

Internet 100%



security and reports levels

- Server web UI is divided to 3 security levels:
 - Local library workers level
 - Local administrator level
 - Master admin level
- Permissions for changing passwords enabling/disabling users and getting reports are distributed accordingly.



What is coming next?

- Authentication will be also possible via other countries ID cards:
 - Finland ID-card
 - Portugal ID-card
 - Belgium ID-card
- Your state may be the next who wants to start using the same successful ID card system. So be ready to provide e-services to state institutions and companies.
- Instead of ID Card is also possible to use other smartcards (like client cards).





Got questions?

Imre Kuus

Sonictest Ltd.

E-mail imre@sonictest.ee

<http://www.sonictest.ee>

Skype: sonictest3