



Role-based Access Control for Securing Dynamically Created Documents

Kaarel Tark

Nortal AS, Estonia
kaarel.tark@nortal.com

Raimundas Matulevičius

University of Tartu, Estonia
rma@ut.ee

Motivation

- ❖ Increasing number of documents
- ❖ Need to secure the document content
- ❖ Display part of document to different stakeholders

Visit nr V2013-12-00014000

Patient's Ambulatory Treatment Record (First visit)

Patient	Name:	Aleksandr Skafandr
	Legal code:	38213123111321
	Age:	30 years
Complaints	head ache in forehead during last 2 days. Striking pain to left arm and elbow. Slept 5-6 hours for the last three weeks period	
Primary diagnosis	R.53.83 - Exhaustion, exhaustive(physical NEC)	
Opinion	Blood pressure high and slept too little. Should go on a regular 8 hour sleeping mode. 1 week in home regime.	
Observations	1 x massage 45min; 1 x term 30min	


.....
Doctor's signature and date

Motivation


- ❖ Increasing number of documents
- ❖ Need to secure the document content
- ❖ Display part of document to different stakeholders

Visit nr V2013-1


Patient's Ambulatory Treatment Record (First visit)



Nurses




Receptionists




Doctors

Patient	Aleksandr Skafandr
	38213123111321
	30 years
Complaints	head ache in forehead during last 2 days. Striking pain to left arm and elbow. Slept 5-6 hours for the last three weeks period
Primary diagnosis	R.53.83 - Exhaustion, exhaustive(physical NEC)
Opinion	Blood pressure high and slept too little. Should go on a regular 8 hour sleeping mode. 1 week in home regime.
Observations	1 x massage 45min; 1 x term 30min

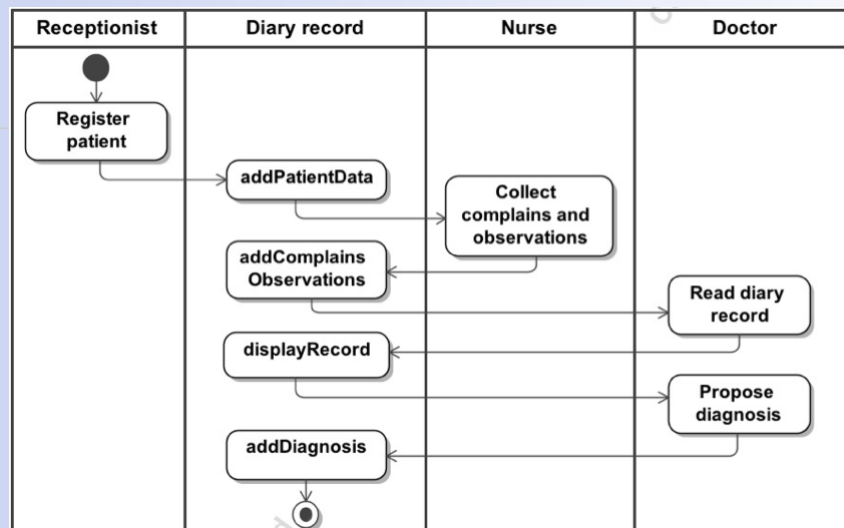


Statisticians

.....
Doctor's signature and date



Doctors



{role= (Eve, Receptionist)}
 {protected=(addPatientData)}
 {right =(Receptionist, addPatientData)}


{role= (John, Doctor)}
 {protected= (displayRecord)}
 {protected= (addDiagnosis)}
 {right = (Doctor, displayRecord)}
 {right = (Doctor, addDiagnosis)}

{role= (Ann, Nurse)}
 {protected=(addComplainsObservations)}
 {right =(Nurse, addComplainsObservations)}

Questions

- ❖ *Can we dynamically define forms and permissions of the document?*
- ❖ *Can we keep the document context complete when applying permissions on documents?*

Demo 1



Dynamic forms


* Role: Nurse



Documents: Refresh

document name	version	XML	Action
Patient diary record	20	208	Edit
Patient diary record	2	209	Edit
Patient diary record	4	210	Edit
Patient diary record	2	211	Edit
Patient diary record	1	212	Edit
Patient diary record	1	213	Edit
Patient diary record	6	214	Edit
Patient diary record	6	215	Edit
Patient diary record	6	216	Edit

Add new Form

document name	xsdId	Description	Action
Patient diary record	101	Diary record	Add new
ExampleApplication	200	Example1 - Application	Add new
Group1	201	Group1 form - Application	Add new
Group2	202	Group2 form - Application	Add new
Group3	203	Group3 form - Purchase order	Add new
Group4	204	Group4 form - Purchase order	Add new
Group5	205	Group5 form - Application	Add new
Group6	206	Group6 form - Purchase order	Add new
Group7	207	Group7 form - Purchase order	Add new
Group8	208	Group8 form - Application	Add new
Group9	209	Group9 form - Application	Add new
ExamplePurchaseOrder	300	Example2 - Purchase Order	Add new

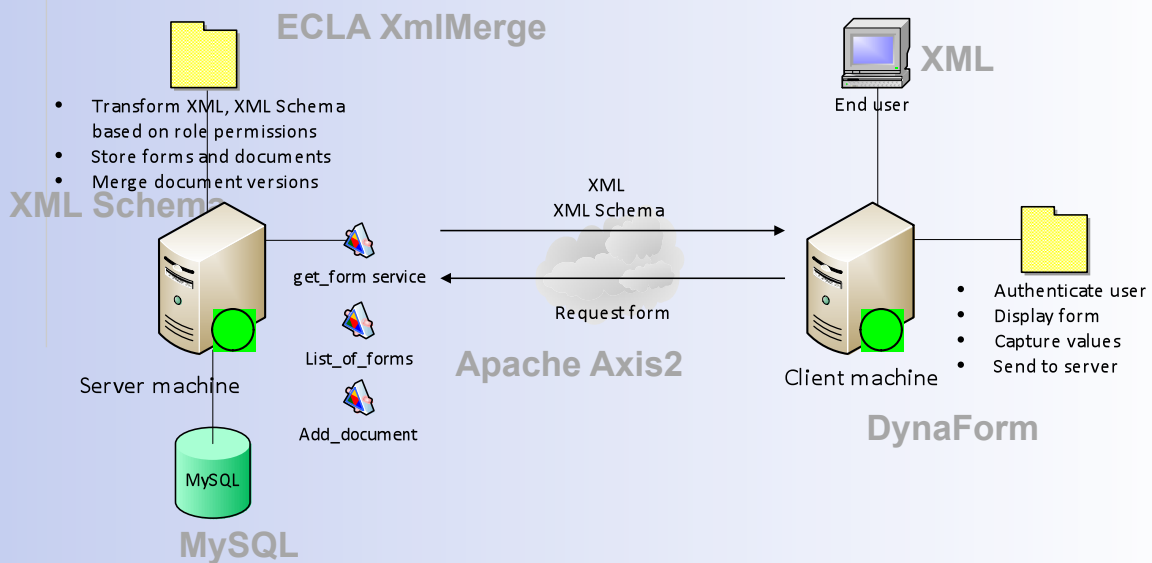


7

2nd Workshop on Security in Business Processes (SBP'13)
26 August, 2013, Beijing, China

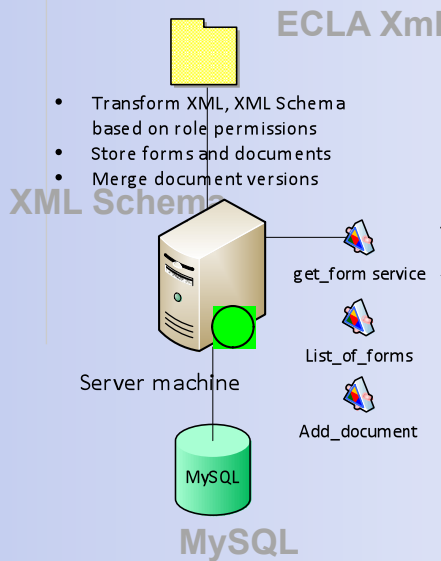
Proposed solution



8

2nd Workshop on Security in Business Processes (SBP'13)
26 August, 2013, Beijing, China

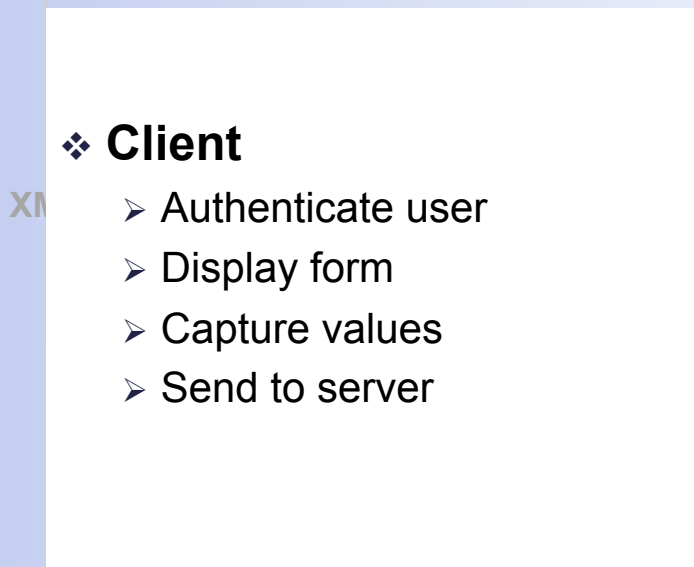
Proposed solution



❖ Server machine

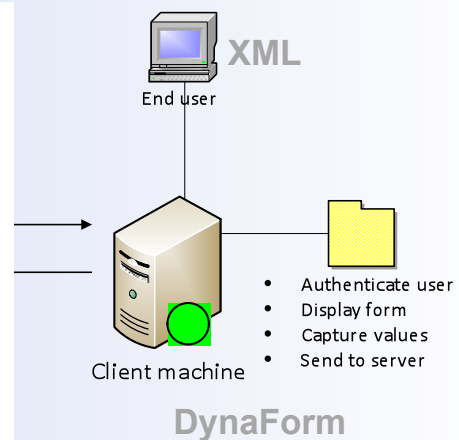
- Transform XML, XML Schema based on role permissions
- Store forms and documents
- Merge document versions

Proposed solution

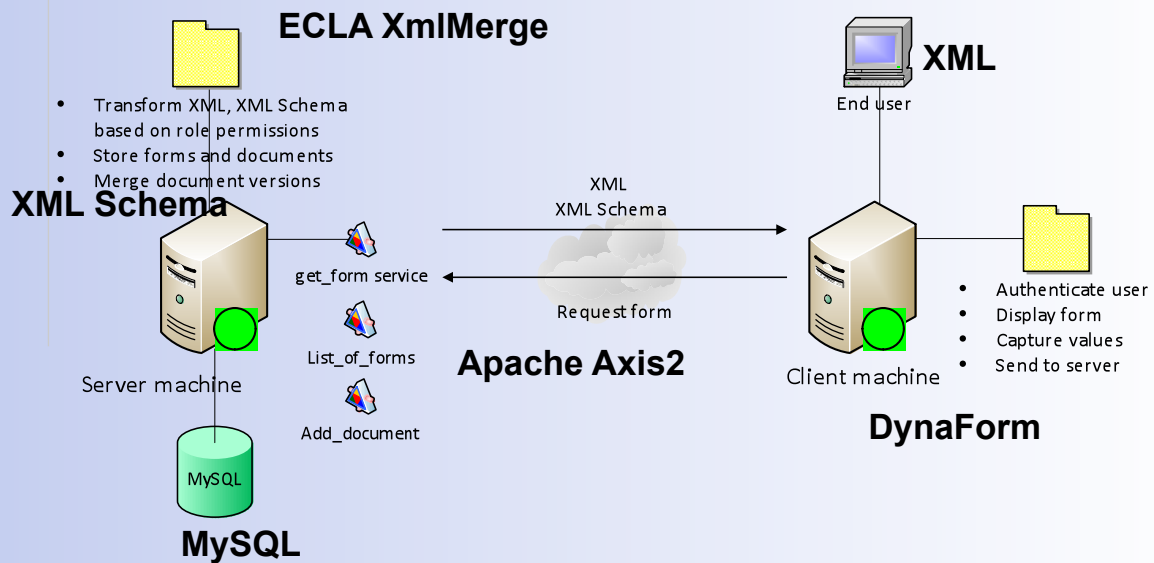


❖ Client

- Authenticate user
- Display form
- Capture values
- Send to server



Proposed solution

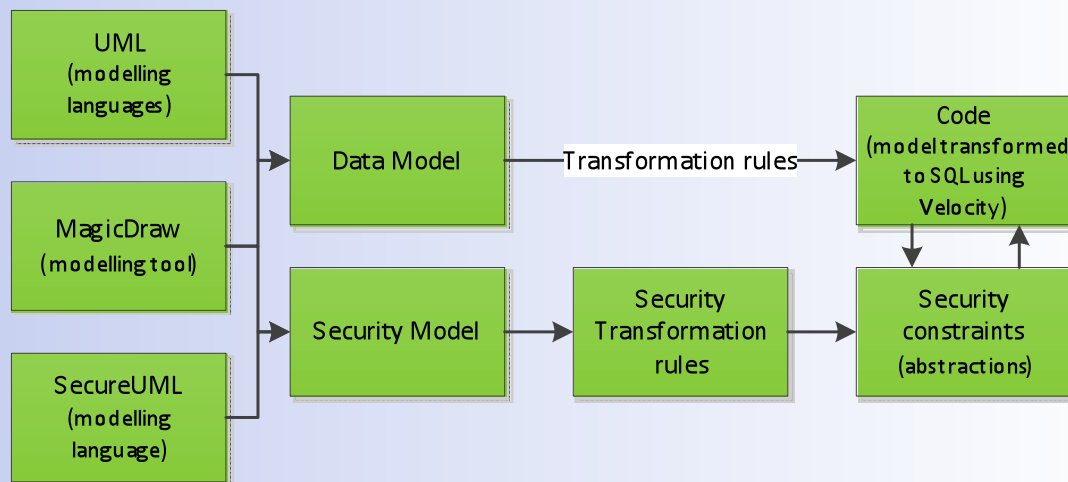


Managing access policy

- ❖ Policy is managed by defining access permissions in the code and then adding the constraints through the database
- ❖ Direct complexity of coding to the complexity of modelling

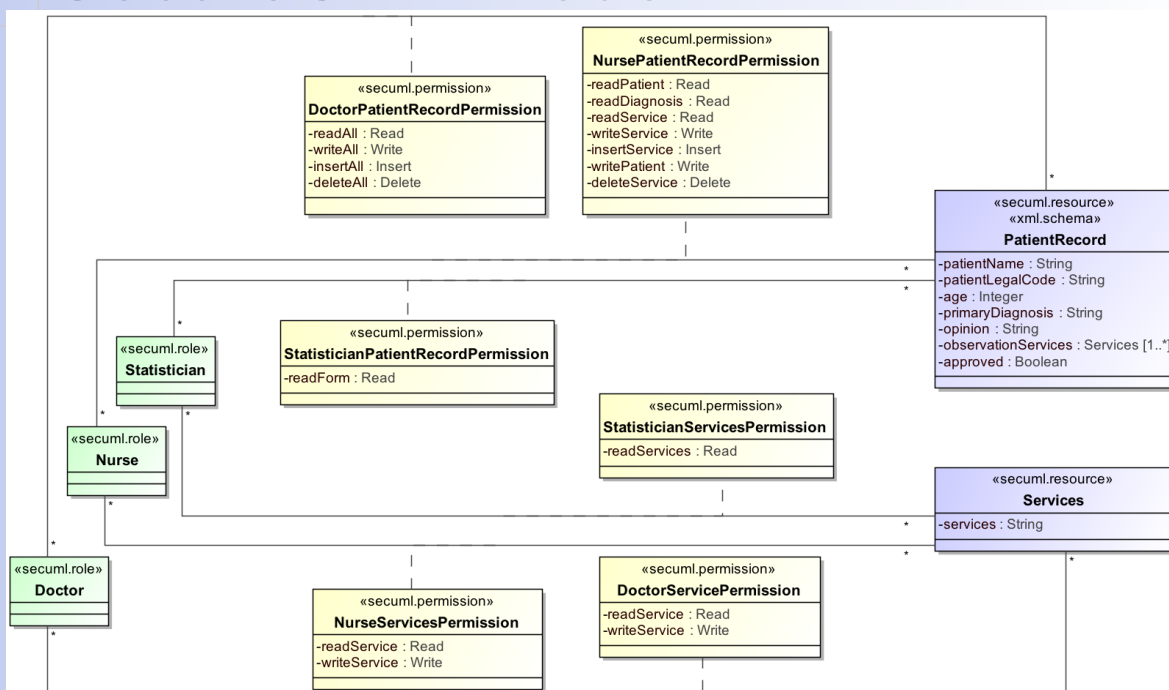
Managing access policy

Model Driven Security

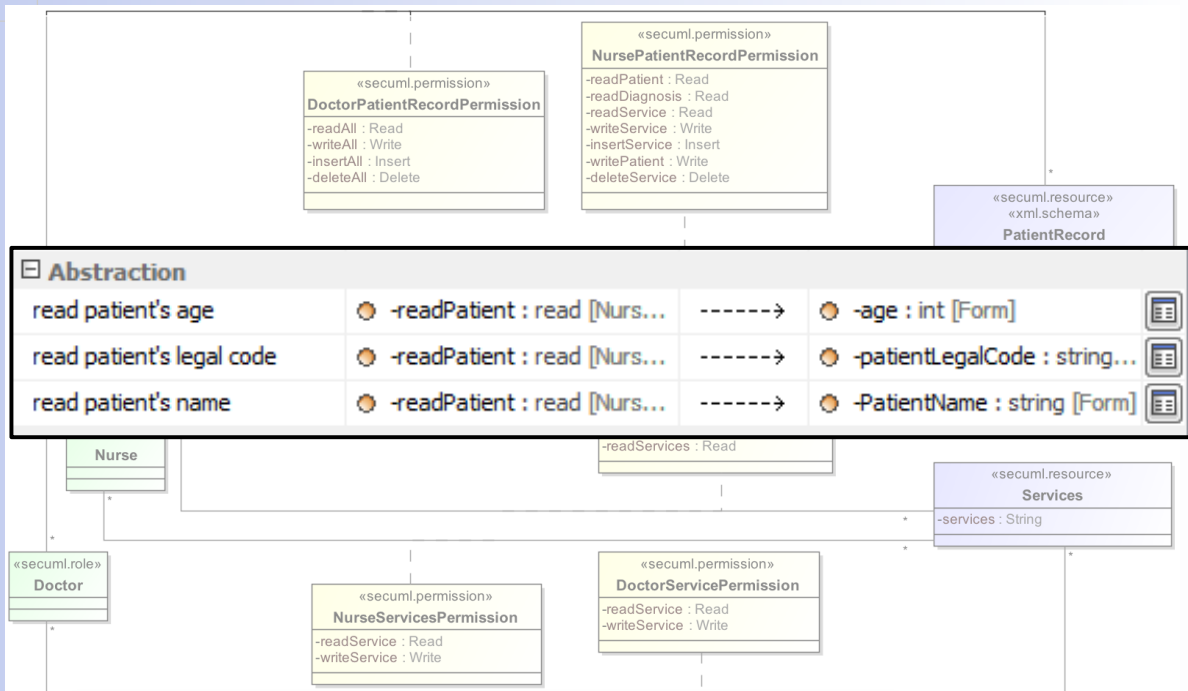


Lodderstedt *et al.*, 2002; Basin *et al.*, 2006

SecureUML model



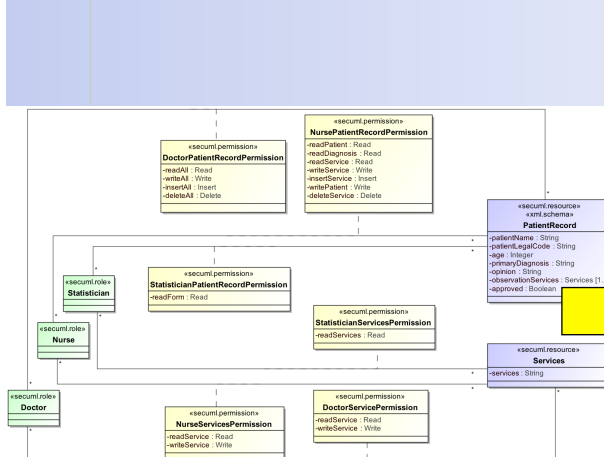
SecureUML model



15

2nd Workshop on Security in Business Processes (SBP'13)
26 August, 2013, Beijing, China

Demo 2



Dynamic forms

* Role: **Nurse**

Documents: **Refresh**

document name	version	XML	Action
Patient diary record	20	208	Edit
Patient diary record	2	209	Edit
Patient diary record	4	210	Edit
Patient diary record	2	211	Edit
Patient diary record	1	212	Edit
Patient diary record	1	213	Edit
Patient diary record	6	214	Edit
Patient diary record	6	215	Edit
Patient diary record	6	216	Edit

document name	xsdid	Description	Action
Patient diary record	101	Diary record	Add new
ExampleApplication	200	Example1 - Application	Add new
Group1	201	Group1 form - Application	Add new
Group2	202	Group2 form - Application	Add new
Group3	203	Group3 form - Purchase order	Add new
Group4	204	Group4 form - Purchase order	Add new
Group5	205	Group5 form - Application	Add new
Group6	206	Group6 form - Purchase order	Add new
Group7	207	Group7 form - Purchase order	Add new
Group8	208	Group8 form - Application	Add new
Group9	209	Group9 form - Application	Add new
ExamplePurchaseOrder	300	Example2 - Purchase Order	Add new

16

2nd Workshop on Security in Business Processes (SBP'13)
26 August, 2013, Beijing, China

Related work

- ❖ Damiani *et al.* (2002)
 - Access control on document type definition
- ❖ Zhang *et al.* (2004)
 - Schema based XML security
- ❖ Seitz *et al.* (2005)
 - Extensible access control language
- ❖ Brucker and Petritsch (2009)
 - Break-glass technique

Answers

- ❖ *Can we dynamically define forms and permissions of the document?*
 - SecureUML
 - Velocity templates
 - MagicDraw
- ❖ *Can we keep the document context complete when applying permissions on documents?*
 - Modifying and merging documents to keep information integrity

Final remarks

- ❖ Limitation
- ❖ Validation
- ❖ Future work

