Model-based Testing of Electronic Passports

Wojciech Mostowski, Erik Poll, Julien Schmaltz, Jan Tretmans, Ronny Wichers Schreur

Electronic Passports

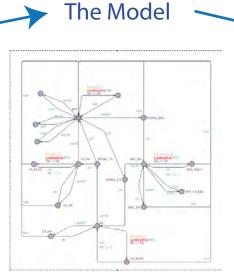
Electronic passports contain a contactless smartcard with a picture and personal data of the holder. New European passports will also contain fingerprints. Several security mechanisms are in place to safeguard the authenticity and confidentiallity of this data. We were involved in a project to test the security in a real-world implementation of the electronic passport.



The Specs



The basic protocols are specified in an ICAO standard. This standard references many other standards. Implementators of the standard have various options in their choice of protocols. Also, the standard is underspecified, in particular for error conditions.



After scrutinising the specifications we constructed a formal model of the passport's behaviour. This model takes the form of a labelled-transition system. The model contains explicit transitions for error conditions.



and any set a set of the set of t	palapart Samatismus - Hit Purchasser
to be desper burt mint he gross he	Do the plan have been been been
	the urber user he say hall a.e.
()- B-O-A/ B # #- B-# #- 7 1986	are below, your min had not but hit
	IN MUP IN .
	es erm. mer in nariski, tali 4-4
and a second sec	IT HIDPL AND THE PRIME HIM & A
" and a first start and a second start and a second start a second start and the second start and	IT ALL STOP, SHUT THE BALT THAT WAS
A supported to the standard and the supported as the support of the support	24 HEDP: SHUT SHI SHI HHE P.3
A DESCRIPTION OF THE PARTY OF T	21 1720, UNIT IN PARTIAL CALL S.S.
a Characteristic Characteristic Contractioners (Contra	all MED, THEY AND THEY AND ANY ANY
and include the form that when the draw formation and the first sector and	23. 4000 (AL) AN AN AN AN AN
W. LINARATIN FLOW ADDRESS AND FLOW ADDRESS AND ADDRESS ADDRESS AND ADDRESS ADDR	2 14 MORT 1417
http://www.ited/fight/http://wited/http://	TO STOR. SALE DO PARTA CALLY S.A.
actionant acts 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1	TO MERT you'l not Yaulian the A.F.
i yeszynamicze (/) i / i szandzieletene	IL OTHER AND IN BHE LACL WIN
ACCOMPANY AND ADDRESS OF THE ADDRESS AND ADDRESS ADDRES	11 HEAT IN THE BE WE A. T
INCOMERCIPACITIES AND IN COMPANY COMPANY	på UPDH, såon be Pacillar-that 8.6
NUMBER OF THE ADDRESS OF THE DESCRIPTION OF THE DES	25 MOP, 1912 But Paulth, SM P.P
 K. Constrained in Laboration of the state of	IN ACCP. DAVE
And and the second	of drips, seen in the call 4.4
WITH DW DW THE READ THAT THE ACCOMPTING AND ADDRESS ADDRES	In which that
THE TRANSPORT OF TARGET A LOT OF MARKED AND TARGET	as bries, pair by pay thill b.b.
	AT 8725- 18-7 BA 88/ 680 0-2
Net Teaming and a section for the section of the se	ar erim ware in warling call a d
AC Press and the Lagrangian of the Control Sector Trains	all secon, part has balled, saw a a
CONTRACT AND DO RECORDING TO AND A DO RECEIPTION OF THE PARTY OF THE P	AL MODEL GALF
ACTORERATIVES FOR THE PROPERTY OF A REPORT OF A	WE STOR. WALT DO BAI 1221. # 1
 International and in the last fields In the second and field (2018) and the last first and the last of the second and first second and the last first second and the last first second and the last of the second and the second and	49 NOP 1411 5-1 84 54 54 5-2
 M 2000 KEY MACRO AND ALL THE APPLICATION CONTRACTOR ADDRESS AND ADDRE ADDRESS AND ADDRESS AND ADDRESS	of the ways on a dail and
And and the fact that the second	an anger that an an an a
100	the strine, where he and that and
Next Diverse Pair (Version CT) - 2 (2 had been CE (2 methods a find a fill a fact of the Editor of a fill a fi	11 MID*, 1817 3-4 44 38 0.0
	Li Mith lart
Recting and and the ball provides of a long processing of the second sec	ter erten entritte mittell des
	or stop- cars and as in c.s.
energy and a second sec	THE MEDIAT SALE
 WY WARANDER STOPPORT See Section 19 and 1 and 19 and 19 and	06 37395 VALT 24 BAC 5411 - 0.#
 - See Section 1 - Construction of the Construction of	17 MESP: Yest Stat Bill JM 4-4
- Case	be arge, seen to be (all 0 a)
months tunned	the MELET AND ANY THE THE A.A.
ADMINISTRATING AND THE ADDITION OF THE REAL PROPERTY AND ADDITIONAL ADDITICICAL ADDITIONAL ADDITICICAL ADDITIO	at MOP, that has set as
	at Mile land
Panetta I	are other, start in maritial daily stat
	as story shit has railed an a
CONTRACTOR OF THE REPORT OF THE REPORT OF THE PROPERTY OF THE	NO OTHE GRAP TH RACING CALL N.R.
	NA RESP. SHUT JAKE PAUSAC SHR. 9.8
	at aron, soit to be rath a p
	HE HELP. YHLT SHE HAD DR. C.L.
	er gran. enty 20 mer (211.4.0
1	States and the law by \$1

The model was fed to the testing tool TorXakis (based on TorX) that automatically generates and executes test cases on the fly. The JMRTD framework provided the Java implementations of the protocols. Also jUnit was employed for *ad-hoc* testing.

Experiences

Understanding the specifications and constructing the model was most of the work. After that using TorXakis to automatically run test cases was quick and easy. We started with a coarse model, which allowed us to run tests early on in the project. The model was then subsequently refined. In this project model-based testing has clearly proven its value.



