Model-based Testing of Electronic Passports

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

Electronic Passports

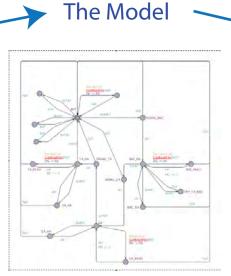
Electronic passports contain a contactless smartcard with a picture and personal data of the holder. New European passports will also contain fingerprints. Several security mechanisms are in place to safeguard the authenticity and confidentiallity of this data. We were involved in a project to test the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



a with the second design of th		pertitionalities. Hit has	
the far despert least finish hat grown indu-	the date of	and hereaf like one	
		In sai tall a.e.	
7+ B+0+4/ B # #+ B-8 #+ 7 1084	on beind: seat	But had not 0.0	
	11 47 m. 1911	In the third, dalls it it	
and the second se	22 402PL 8813	Test warmed, man e .e.	
and the second se	13. UT3P: UR1.	THE BALL LACT B. M.	
eff fanlagten (jann rigers annen i riger genande), 6 4. jiblinsipen par 5. den jis en de ann	DA HOUP'S SHEET	545 BBL 498 9-3	
Represented to provide the second s		In Persiler cpl. 8-8	
 Sectorements (AMP scale) (2) and (2) and		the Period and a r	
 ar (a) present of the state of the first of the state of		IN THE LAST WH	
 Comparison of the Application Plant Comparison of the Network Comparison of The Plant Com	1 mil 10	ALC: BAL (# 9.8)	
K. DELENSTER STRUCTURE CONCIDENT TO A LOCAL STRUCTURE CONTINUES. IN A DESCRIPTION OF THE STRUCTURE CONTINUES. Kent Transmitted Preservice Continue (National Continues)		IN PATRAC RAIL S.A.	
An in considerant and a first state of the local state of the second state of the seco		In Parallel Gall B.B.	
 Methods and a state of the stat		the Particle of a later	
A THE REPORT OF A DESCRIPTION OF A DESCR		THE RELEASE A.	
Incompared to the second s	an union one	the Pacillar real dis-	
NAME AND ADDRESS OF A DREAM OF A	1 10. 10.	But Paulth and h.b.	
A Destruction of the Officer Division	IN MUR. MUT		
A COMPARED IN LODIER AND A DESCRIPTION OF A DESCRIPTION O		In Tel (all 4.4	
A DESCRIPTION OF THE ADDRESS OF THE	In state and	Test that was a s	
	to which the		
Read Comparison of	44 17241, 1812	Dr par 1917 b.b	
N (WARRENT NOT WEARING MET YOR CONTRACT OF A DRIVEN AND THE ADDRESS AND THE AD		and and date 2-2	
h helpenministelen til prisiden		To Varible, call 8-4	
 ACPression of the Learning of CPU Inscite Time 		THE PALINE WH & R.	
COLUMN TO THE REPORT OF THE RE	AL 4037 344		
		Dr 841 1913 9-5	
 Next Your Add Control of The Add Party of Th		Set 84 36 4-8	
 K 2000 K21 K22 CALANDER LET TURY LET LOS K 2000 KKT SHERCHARD 2000 CP1 KK Mc2 Mathematical LET Calander Calander 		Dr. 14, 1975 (0.4)	
Providence of the second	AN AUGUST 184.1		
Text Design (%), (where \$1), (%), (%), (%), (%), (%), (%), (%), (%		The set which a d	
and the second of the second o	LL MUN, MAR	201 10,00 10.0	
Kanada and Alaba		the set data is a	
And A state of the Contract of the Contract of the London State of the State of the Contract o	La serie inte	And the lot of the lot	
Research Control of Co	the same lines		
A WINTALLAL COLUMN		by har tall & d	
and press to press the press of		Test 510 (8) 5.4	
h. 400	out erge. start	The start (at) is in	
- Management	Th #82371 ABL7	Bot 242 16 9.8	
EXCELOSE TAXABLE FOR TAXABLE F		Dr. Ball Latt. B.A.	
BRAINBARD AND THE AND THE AND THE PARTY OF AND THE AND		Sun 244, 1841 (1.9	
b Streatersenation (https://www.sectorsenaters/Systematics/Systemat Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systematics/Systema	at MUP- Serie		
C. Principal		In variable, dall is de-	
		The PALLER AN A .	
		Do RACIMAL CALL M. M.	
e .0m	NO NEOPI INCO	SHI FALSAC NR. 1.8	
	AT 1729, 1611	In the cars a p	
		Sec. 847, 18, 4, 8	
	an arget sats	20 BH (411.0.0	
	the state and		

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.



