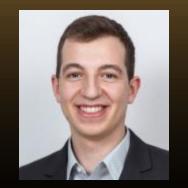
Self-labeling Electronic Shelf Labels Pwning the Next Big Thing in Retail



Title: Self-Labeling Electronic Shelf Labels. | Responsible: S. Robertz | Version / Date: V1.0/2022-06 | Confidentiality Class: public © 2022 SEC Consult | All rights reserved

an atos company

About Me



Steffen Robertz Security Consultant

s.robertz@sec-consult.com LinkedIn:<u>shr70</u>

SEC Consult Unternehmensberatung GmbH Leopold-Ungar-Platz 2/3/3 1190 Vienna, Austria

www.sec-consult.com

Research conducted at the SEC Consult Vulnerability Lab

Title: Self-Labeling Electronic Shelf Labels. | Responsible: S. Robertz | Version / Date: V1.0/2022-06 | Confidentiality Class: public © 2022 SEC Consult | All rights reserved



What's an ESL tag? Parts

- Display (e.g. E-Ink)
- Usually Battery powered, supposed to last multiple years
- Some method of wireless communication (Bluetooth LE, NFC, 433 MHz)
- A matching transceiver for a regular computer







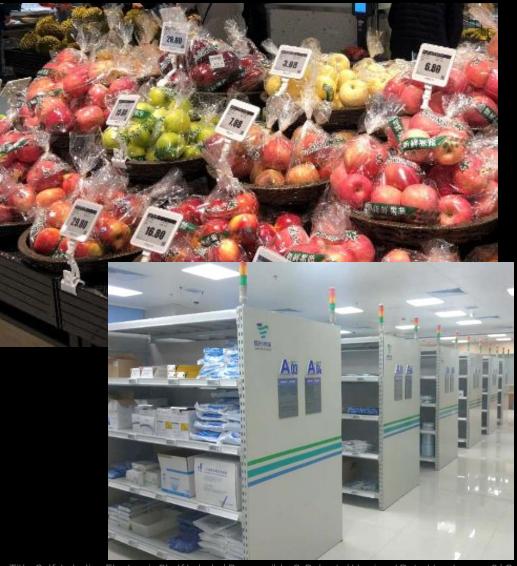
ESL Tags Is It Really the Next Big Thing?

- ESL market worth 855 Million \$ in 2021 [1]
- Estimate for 2022: 980 Million \$ [1]
- 2032: 5.2 Billion \$ [1]
- Convenient price changes
- Promotional offers can be communicated easily
 - Attention drawn by e.g. flashing lights
 - Influences consumers decision

[1]: https://www.prnewswire.co.uk/news-releases/electronic-shelf-label-market-to-reach-usd-5-2-bn-by-2032-latest-fact-mr-study-834855956.html



ESL Usage



Title: Self-Labeling Electronic Shelf Labels. | Responsible: S. Robertz | Version / Date: V1.0/2022-06 | Confidentiality Class: public © 2022 SEC Consult | All rights reserved



SEC Consult

an atos company

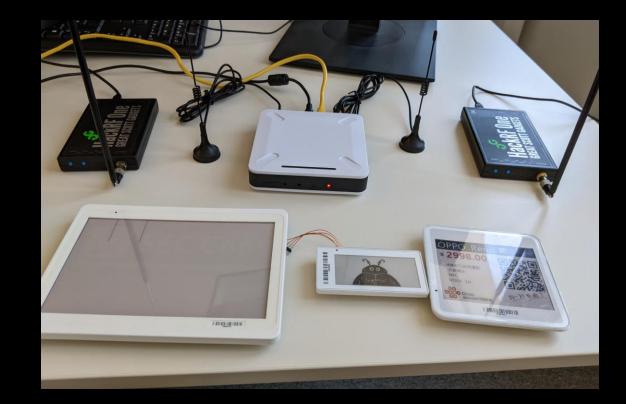
ESL Usage Attack Scenarios

- Obstruct retailer -> blackmail for ransom
- Phishing site as QR code for discount coupons
- Maker community: Cheap display with long battery lifetime



ESL Usage The Test Setup

- Common Chinese ESL tag supplier
- AP/Basestation, connected via Ethernet
- Tags connected via 433 MHz to Basestation
- Our Station: Retail Flavor
 - Also available as Industrial Flavor
- Tags available in multiple sizes (1.5" to 11.6")
- Attacker: Using multiple HackRF for receiving and sending custom data frames



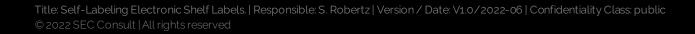


an atos company

ESL Usage The Design Tool

- Tool can create pixel graphics
- Tag field stores list of tags to update
- Status box in lower right-hand corner gives status information after transmission is completed
- Also available: .NET SDK for custom projects
- POS integration

ArtiColor: False FortFamily: SmSun FortStyle: Regular Alignment: Left Rectangle:W 0 H 0 Trans VarKey: FormatFlags: NoClo ImageType: R 127 G 127 B 127 Gray 127 R 127 G 127 B 127 Gray 127 Excel Cancel Save SaveA	ET ₀	Pix Templ	ate D	esgin										-		<
Tag Stat: 142 230 200 1200 notate LED Tag Color: Red Image Tag Template Sample ESL200R Image 1 Image	15	4:200*200,	213:1	04*212	; 290:128*296; 420:30	0*400; 750:3	84*640; 1250	:652*492					Item Type:	Image		_
Tag Templete Sample ESL250R To: [1] To: [1] T	Tag	g Size:	154		213 290	420	750	1250	Rotate	LED	Tag Color:	Red 🗸		_		=
D Type X Y VerValue FortSize ArtiColor FortSiye Regular Narris 1 C-Ubers/VertetLiv Signores/Social 2002/01/2012 VerValue Norksyn 0 Image 1 C-Ubers/VertetLiv Signores/Social 2002/01/2012 VerValue 0 Image 1 C-Ubers/VertetLiv FortSize Image 0 Image 1 C-Ubers/VertetLiv FortSize Migment 0 Image 1 C-Ubers/VertetLiv FortSize Migment 0 Image 1 C-Ubers/VertetLiv FortSize ArtiColor FortSize 0 Image 1 C-Ubers/VertetLiv FortSize ArtiColor FortSize 0 Image 1 C-Ubers/VertetLiv FortSize ArtiColor FortSize ArtiColor FortSize 1 C-Ubers/VertetLiv FortSize ArtiColor FortSize ArtiColor FortSize Tog Stoce 1 C-Ubers/VertetLiv Image False Smissin Regular Left Bock		T 1.		1.50	2000									 -		_
D Type X Y VarValue FortSize ArtiColor Fortsize FortSize <td< td=""><td></td><td>g remplate</td><td>e Samp</td><td>DIE:ESL</td><td>.290R</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>/alue格式[ori</td><td>ce Scrint 🖂</td><td>(木</td></td<>		g remplate	e Samp	DIE:ESL	.290R									/alue格式[ori	ce Scrint 🖂	(木
D Type X Y VerValue FortSize ArtColor FortSize Tanus D Type X Y VerValue FortSize ArtColor FortSize Tanus D Type X Y VerValue FortSize ArtColor FortSize Tanus D Type X Y VerValue FortSize ArtColor FortSize Tanus D Type X Y VerValue FortSize ArtColor FortSize Tanus D mage 1 1 Cubers/Perteet/ mage Fale SmSun Regular Alexande D mage 1 1 Cubers/Perteet/ mage Fale SmSun Regular Left Black 00/Transper D mage 1 1 Cubers/Perteet/ mage Fale SmSun Regular Left Black 00/Transper D mage 1 1 Cubers/Perteet/ mage Fale SmSun Fale Fale				2									大小k偏移 y	偏移分隔标		+
ID Type X Y VarValue FortSize ArtiColor FortSize FortSize <t< td=""><td></td><td></td><td></td><td></td><td>00.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>VarValue:</td><td>C:\Users\P</td><td>entest\Des</td><td>kto</td></t<>					00.								VarValue:	C:\Users\P	entest\Des	kto
ID Type X Y VarValue FortSize AntiColor FortSize AntiColor FortSize FortSize Refresh(F5.Erter) ID Type X Y VarValue FortSize AntiColor FortSize Refresh(F5.Erter) ID Type X Y VarValue FortSize AntiColor FortSize Refresh(F5.Erter) ID Type X Y VarValue FortSize AntiColor FortSize Refresh(F5.Erter) ID Type X Y VarValue FortSize AntiColor FortSize Refresh(F5.Erter) ID Type X Y VarValue FortSize AntiColor FortSize Refresh(F5.Erter) ID Type X Y VarValue FortSize AntiColor FortSize Refresh(F5.Erter) ID Type X Y VarValue FortSize AntiColor FortSize Refresh(F5.Erter) Externed Externed <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>FontSize:</td><td>Image</td><td></td><td>_</td></td<>													FontSize:	Image		_
ID Type X Y VarValue FortSam FortSam FortSam ID Type X Y VarValue FortSize ArtiColor FortSam FortSam FortSam ID Type X Y VarValue FortSize ArtiColor FortSam FortSam FortSam ID Type X Y VarValue FortSize ArtiColor FortSam			P	5	T S								FontColor:	Black		~
ID Type X Y Var/aue Fort.Size ArtiColor Fort.Size ArtiColor Fort.Size ArtiColor Fort.Size													AntiColor:	False		`
ID Type X Y VarValue Fort Size ArtiColor Fort Family Fort Siyle Alignment Fort Size Refresh(F5.Enter) ID Type X Y VarValue Fort Size ArtiColor Fort Family Fort Siyle Alignment Fort Color Retacting E 0 Image 1 C. Ubero VPentest \ Image False SimSun Regular Left Black 00/Transpærer 2 1 C. Ubero VPentest \ Image False SimSun Regular Left Black 00/Transpærer 2 1 C. Ubero VPentest \ Image False SimSun Regular Left Black 00/Transpærer 2 1 <td></td> <td>FontFamily:</td> <td>SimSun</td> <td></td> <td>~</td>													FontFamily:	SimSun		~
ID Type X Y Var/alue FortSize ArtiColor FortSayle Alignment FortColor Retangle W 0 H0 Trans. \\ Var/alue ID Type X Y Var/alue FortSize ArtiColor FortSayle Alignment FortColor Retangle W 0 H0 Trans. \\ Var/alue 0 Image 1 C.\Llsenv.Ventest Image Faise Sim Sun Regular Left Black 000Transpare 20 Image 1 C.\Llsenv.Ventest Image Faise Sim Sun Regular Left Black 000Transpare 20 Image 1 C.\Llsenv.Ventest Image Faise Sim Sun Regular Left Black 000Transpare 20 Image 1 Image Faise Sim Sun Regular Left Black 000Transpare 20 Image 1 Image Faise Sim Sun Regular Left Black 000Transpare 20 Image Image Faise													FontStyle:	Regular		~
ID Type X Y VarValue FortSize AntiColor FortFamily FortSiyle Alignment FontColor Rectanjle Image Tag: D56666 D56666 FortSize AntiColor FortFamily FortSiyle Alignment FontColor Rectanjle Image Tag: D56666 D56666 FortSize AntiColor FortFamily FortSiyle Alignment FontColor Rectanjle Image Tag: D56666 D56666 FortSize AntiColor FortSize													Alignment:	Left		~
ID Type X Y VarValue Fort Size ArtiColor Fort Siyle Alignment Fort Color Rectangle 0 Image 1 1 C:\Users\Pentest\ Image Faile SimSun Regular Left Black 000Transpare 0 Image 1 1 C:\Users\Pentest\ Image Faile SimSun Regular Left Black 000Transpare 0 Image 1 1 C:\Users\Pentest\ Image Faile SimSun Regular Left Black 000Transpare 0 Image 1 1 C:\Users\Pentest\ Image Faile SimSun Regular Left Black 000Transpare 058686 Power: 2.9 RSSI: 28 Temp: 25 Result: Success Station returned result data[14] Station: 14 BatchCode d372 TaglD: 28 Temp: 25 Result: Success Station returned result data[14] Station: 14 BatchCode d372 TaglD: 28 Temp: 25 Result: Success Station returned result data[14] Station: 14 BatchCode d372 TaglD: 25 Result: Success Station: 14 BatchCode d372 TaglD: 25 Result: Success Station: 14 BatchCode d372 TaglD: 25 Result: Success Station: 14 BatchCode d372 TaglD: 25 Result: Success <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Rectangle:W</td><td>0 H 0</td><td>Transp</td><td>~</td></t<>													Rectangle:W	0 H 0	Transp	~
ID Type X Y VarValue FontSize AntiColor FontSiyle Alignment FontColor Rectangle 0 Image 1 1 C:\Users\Penteet\ Image False SimSun Regular Left Black 0/0/Transpare 2 1 C:\Users\Penteet\ Image False SimSun Regular Left Black 0/0/Transpare 2 1 C:\Users\Penteet\ Image False SimSun Regular Left Black 0/0/Transpare 2 1 C:\Users\Penteet\ Image False SimSun Regular Left Black 0/0/Transpare 2 1 1 C:\Users\Penteet\ Image False SimSun Regular Left Black 0/0/Transpare 2 1 1 C:\Users\Penteet\ Image False SimSun Regular Left Black 0/0/Transpare 2 1 1 C:\Users\Penteet\ Image False SimSun Regular Left Black 0/0/Transpare 2 Realt: Succes Saton retume													VarKey:			~
ID Type X Y VarValue Fort.Size AntiColor Fort.Siyle Alignment Font.Color Rectangle 0 Image 1 1 C:\Users\Pertest\ Image Faise SimSun Regular Left Black 000Transparer 0 Image 1 1 C:\Users\Pertest\ Image Faise SimSun Regular Left Black 000Transparer 0 Image 1 1 C:\Users\Pertest\ Image Faise SimSun Regular Left Black 000Transparer 058666 Fourt.Size AntiColor Fourt.Size AntiColor Fourt.Size Tag: 058666 058666 Fourt.Size AntiColor Fourt.Size Image Faise SimSun Regular Left Black 000Transparer 058666 Fourt.Size Image Faise SimSun Regular Left Black 000Transparer 058666 Fourt.Size Image Faise SimSun Regular Left Black 000Transpa													FormatFlags:	NoClip		~
ID Type X Y VarValue FontSize AntiColor FontStyle Alignment FontColor Rectangle 0 Image 1 1 C:\Users\Pentest\ Image False SimSun Regular Left Black 0/0/(Transpare) 25 Feastl: Success Sand Result: Success Sand Result: Success Sand Result: Success Sand Result: Success 4 4 4 4 4 4 4 4 4 14 Station: returned result data [14] Station: returned result data [1													ImageType:			~
ID Type X Y VarValue FontSize AntiColor FontStyle Alignment FontColor Rectangle 0 Image 1 1 C:\Users\Pentest Image False SimSun Regular Left Black 0/0/Transpare 0 Image 1 1 C:\Users\Pentest Image False SimSun Regular Left Black 0/0/Transpare 0 Image 1 1 C:\Users\Pentest Image False SimSun Regular Left Black 0/0/Transpare 0 Image 1 1 C:\Users\Pentest Image False SimSun Regular Left Black 0/0/Transpare 0 Image 1 1 C:\Users\Pentest Image False SimSun Regular Left Black 0/0/Transpare 05B6B6 Power: 2.9 RSSI: :28 Temp: 25 Regult: Success Staton:: 14 BatchCode: 0/712 TagID: 05B6B6 Power: 2.9 RSSI: :28 Temp: 25 Regult: Success Sentor: 14 BatchCode: 23483 TagID: 05B6B6 Power: 2.9 RSSI: :30 Temp: 25 Regult: Success </td <td></td> <td>R 127 G 12</td> <td>7 B 127</td> <td>Gray 127</td> <td>ī</td>													R 127 G 12	7 B 127	Gray 127	ī
ID Type X T Varvalue PontSize AntiColor PontSize													Cancel		Excel	
0 Image 1 C:\Users\Pentest\ Image False SimSun Regular Left Black 0/0/Transparer 0 Image 1 C:\Users\Pentest\ Image False SimSun Regular Left Black 0/0/Transparer 0/56B6B Power: 2.9 RSSI: -28 Temp: 25 Result: Success 2 1 1 SimSun Regular Left Black 0/0/Transparer 0/56B6B Power: 2.9 RSSI: -28 Temp: 25 Result: Success 2 1 1 SimSun Regular 1 1 SimSun		Type	x	Y	VarValue	FontSize	AntiColor	FontFamily	FontStyle	Alianment	FontColor	Rectangle	Tag: 05B68	36		^
25 Result: Success Send Result: Success Station returned result data:[14] Station: 14 BatchCode 60712 TagID: DSB686 Power: 2.9 RSSI: -28 Temp: 25 Result: Success Send Result: OK Station: 14 BatchCode 60712 TagID: DSB686 Power: 2.9 RSSI: -28 Temp: 25 Result: Success Send Result: OK Station: 14 StatchCode 627483 TagID: 058686 Power: 2.9 RSSI: -30 Temp: 25 Result: Success Station: 15CF[14 v] Station: 15CF[14 v]														r: 2.9 BSCI-		~
Station returned result data:[14] Station: 14 Batch:Code 60712 TapID: 05B686 Power: 2.9 RSSI: -28 Temp: 25 Result: Success Send Result. OK Station: returned result data:[14] Station: 14 Staticnate 40714 Station: 14 Staticnate 714 Station: 14 Staticnate 714 Station: 14 Staticnate 714 Station: 15CF[14 v] Station:													25 Result: Suc	cess	zo remp.	Î
058686 Power: 2.9 RSSI: -28 Temp: 25 Result: Success Send Result: OK Station: returned result data:[14] Station: 14 BatchCode:23483 TagID: 036686 Power: 2.9 RSSI: -30 Temp: 25 Result: Success Station: 15CF[14 v) Station:													Station returne	d result data	[14]	
Send Result: OK Station returned result data:[14] Station: 14 Batch/Code:23483 TagID: 0056686 Power: 2.9 RSSI: 30 Temp: ZS Result: Success Station: 15CF[14 ~ V]													05B6B6 Powe	r: 2,9 RSSI: -		
Station: 14 BatchCode:23483 TagID: USB686 Power: 2.9 RSSI: -30 Temp: ZS Result: Success Station: 15CF[14] Station: 15CF[14]													Send Result: (DK		
05B686 Power: 2,9 RSSI: -30 Temp: 25 Result: Success Station: 15CF[14 V Send													Station returns	1. 1. 1. 1. 1.		
Station: 15CF/14 V Send																
													Station: 14 Ba 05B6B6 Powe	tchCode:234 r: 2,9 RSSI: -	83 TagID:	~
													Station: 14 Ba 05B6B6 Powe 25 Result: Suc	tchCode:234 r: 2,9 RSSI: - ccess	83 ŤagID: 30 Temp:	Ĵ





The Hardware

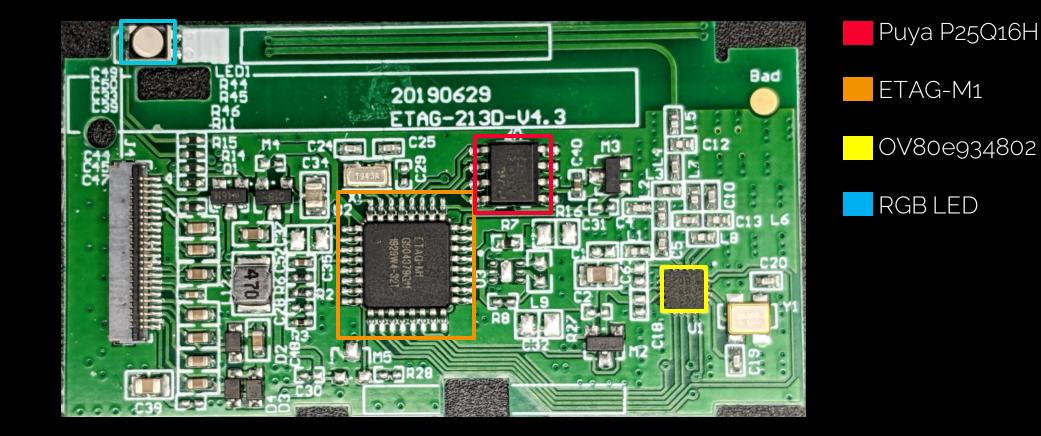


Title: Self-Labeling Electronic Shelf Labels. | Responsible: S. Robertz | Version / Date: V1.0/2022-06 | Confidentiality Class: public © 2022 SEC Consult | All rights reserved

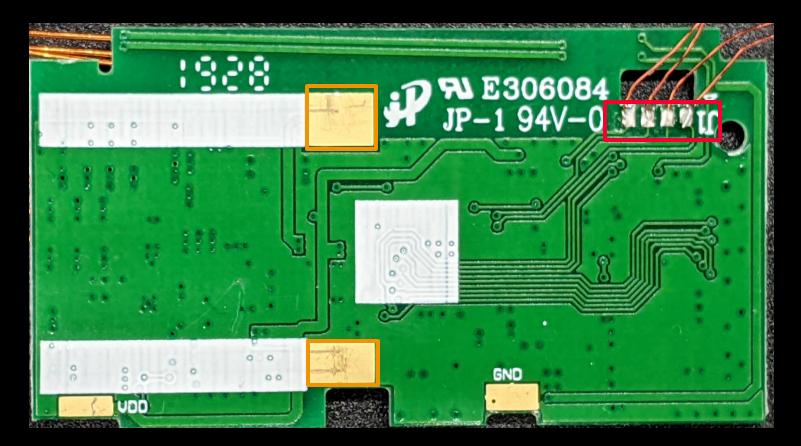
an atos company



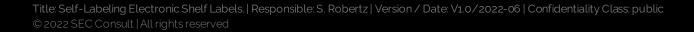








Battery Connector
Debug Header

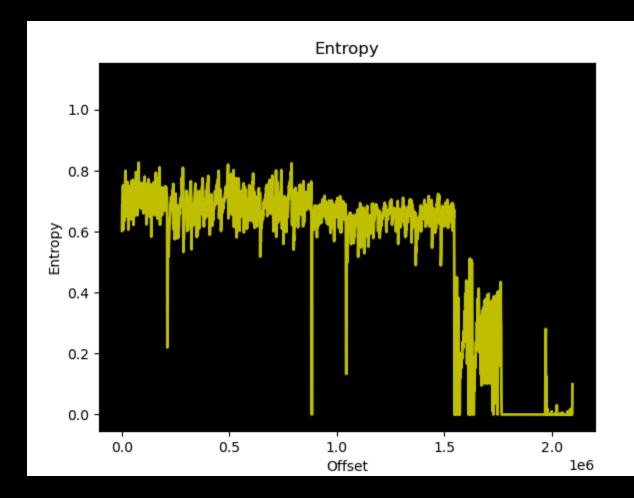






The Tag External SPI Flash

- 2 MB of Flash storage
- Image data starts at 0x1e1000
- First black color channel, then red
- Image stored in rows
- Beginning of Flash contains something else
 - Most likely firmware
- Python script that parses images from flash dumps will be published









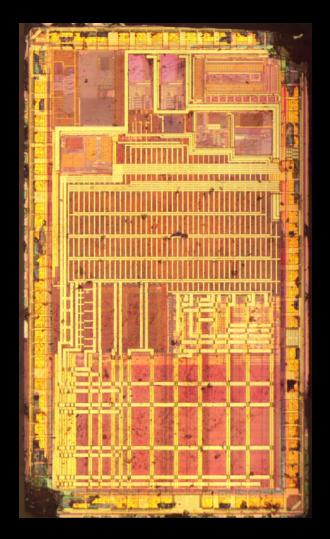
The Tag Identifying the E-Tag M1

	 32 unknown 31 XTAL1 30 XTAL2 29 VCC 28 Flash_MISO 26 Flash_MOSI 25 Flash_CLK 	
SWIM 1 Reset 2 unknown 3 unknown 4 GND 5 VCC 6 VCC 6 unknown 7 unknown 8	, O E-Tag M1	24 Flash_Powersafe 23 unknown 22 unknown 21 unknown 20 LED3 19 LED2 18 Display3 17 Display2
	RF1 9 RF2 10 RF2 11 RF5 11 RF5 11 RF5 11 RF5 11 LED1 15 LED1 16	



The Tag Identifying the E-Tag M1

- Boiling the Chip in 95% concentrated sulfuric acid
 - Removes the epoxy packaging
- IC is cleaned with Isopropanol.
- Manufacturer marking is visible





The Tag The E-Tag M1 MCU

- Manufactured by ST Microelectronics
- Likely designed or produced in 2010
- R758R, might be ST internal part number?







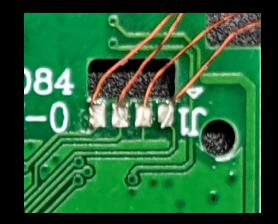
- Backside of PCB has 4 testpads that look like debug access
- Pin 1: MCU Pin 2
- Pin 2: GND
- Pin 3: MCU Pin 1
- Pin 4: VDD

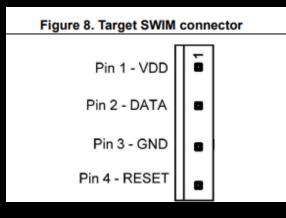




The Tag Debug Access

- Backside of PCB has 4 testpads that look like debug access
- Pin 1: MCU Pin 2
- Pin 2: GND
- Pin 3: MCU Pin 1
- Pin 4: VDD
- STM8 SWIM debug header
 - Pin 1 is just marked on the wrong side
 - Pin 1: RESET
 - Pin 3: DATA
- Confirm RESET by pulling pin low and checking if the tag restarts







The Tag Debug Access

- Use stm8flash with ST-Link V2
- Use any STM8, preferably with much Flash and RAM
 - Start addresses seem to be consistent across all versions
- stm8flash -c stlinkv2 -p stm8s2081b -s 0x8000 -b
 131072 -r dump
 - Indicates 64kByte Flash
 - ROP seems to be activated
- Using same method:
 - 2048 Bytes EEPROM

0000ff90:	7171	7171	7171	7171	7171	7171	7171	7171	адададададададада
0000ffa0:	7171	7171	7171	7171	7171	7171	7171	7171	адададададададада
0000ffb0:	7171	7171	7171	7171	7171	7171	7171	7171	адададададададада
0000ffc0:	7171	7171	7171	7171	7171	7171	7171	7171	адададададададада
0000ffd0:	7171	7171	7171	7171	7171	7171	7171	7171	адададададададада
0000ffe0:	7171	7171	7171	7171	7171	7171	7171	7171	адададададададада
0000fff0:	7171	7171	7171	7171	7171	7171	7171	7171	адададададададада
00010000:	0000	0000	0000	0000	0000	0000	0000	0000	
00010010:	0000	0000	0000	0000	0000	0000	0000	0000	
00010020:	0000	0000	0000	0000	0000	0000	0000	0000	
00010030:	0000	0000	0000	0000	0000	0000	0000	0000	





The Tag Debug Access: Finding the Unique ID

- Multiple known addresses for unique ID
 - 0x48CD
 - 0x4865
 - 0x4926
- Only 0x4926 returned data that would fit the format of Table 14
- Hence:
 - X co-ordinate: 31
 - Y co-ordinate: 58
 - Wafer number: 22
 - Lot number: G904379
- According to STM Forums, 0x4926 seems to be unique to STM8L devices

	Tabl	e 14. U	nique I	D regist	ters (96	bits)							
Address	Content description				Unique	e ID bits							
		7	6	5	4	3	2	1	0				
0x48CD	X co-ordinate on	U_ID[7:0]											
0x48CE	the wafer	U_ID[15:8] U_ID[23:16]											
0x48CF	Y co-ordinate on												
0x48D0	the wafer	U_ID[31:24]											
0x48D1	Wafer number	U_ID[39:32]											
0x48D2		U_ID[47:40]											
0x48D3]				U_ID[55:48]							
0x48D4	1				U_ID[63:56]							
0x48D5	Lot number				U_ID[71:64]							
0x48D6	1				U_ID[79:72]							
0x48D7	1				U_ID[87:80]							
0x48D8	1				U_ID[95:88]							





- Factory is Alibaba Gold Plus Supplier
 - Alibaba produces a production line verification report
 - Contains all fabrication machines of the factory
- List contains "Ultrasonic Fuse"
 - STM8L are custom bonded
 - Unique pinout
 - Should still be traceable through STM Lot numbers
 - "Ultrasonic Fuse" could also be for sealing the casing (ultrasonic welding of plastics)



The RF Protocol



Title: Self-Labeling Electronic Shelf Labels. | Responsible: S. Robertz | Version / Date: V1.0/2022-06 | Confidentiality Class: public © 2022 SEC Consult | All rights reserved

an atos company

2 2

The RF Protocol Gaining Insights From FCC Files

Equipment	Station
Trade Mark	N/A
Model Name	ETAP01
Serial No.	ETAP
Model Difference	All models have the same functionality, software and electronics, only the color, front frame shape and model names may differ. Test sample model: ETAP01
FCC ID	2ARJ5-ETAP01
Antenna Type	Suction cup Antenna
Antenna Gain	5dbi
Frequency Range	433.92MHz
Number of Channels	1
Modulation Type	GFSK
Battery	N/A
Power Source	AC 120V 50Hz from adapter
Adapter Model	MODEL NO. :GS12E05 INPUT:100-240V~,50/60Hz, 0.31A
	OUTPUT:5V 2.0A

FCC Info Basestation

2.2 GENERAL DESCRIP	TION OF EUT
Equipment	Etag
Trade Mark	N/A
Model Name	ET0213
Serial No.	ET0290
	All models have the same functionality, software and
Model Difference	electronics, only the color, front frame shape and
	model names may differ. Test sample model: ET0213
FCC ID	2ARJ5-ET0213
Antenna Type	PCB Antenna
Antenna Gain	1.0dbi
Frequency Range	433.92MHz
Number of Channels	1 1
Modulation Type	ASK
Battery	N/A
Power Source	DC 3.0V from battery
Adapter Model	N/A

FCC Info ESL Tag



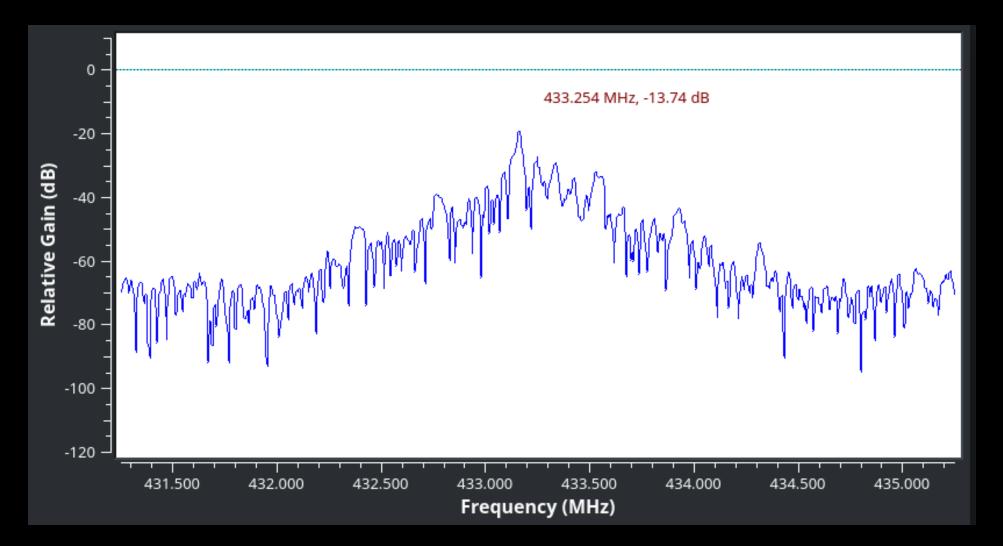
Title: Self-Labeling Electronic Shelf Labels. | Responsible: S. Robertz | Version / Date: V1.0/2022-06 | Confidentiality Class: public © 2022 SEC Consult | All rights reserved

The RF Protocol Gaining Insights From FCC Files

- FCC test lists different modulations for tag and base station
- FCC files list one channel at 433.92MHz
- Manual talks about frequency hopping technology for anti-jamming
 - Was never observed
 - Violation of the one channel/one frequency statement

24

The RF Protocol Finding the Right Frequency





Live Demo Replay Attack

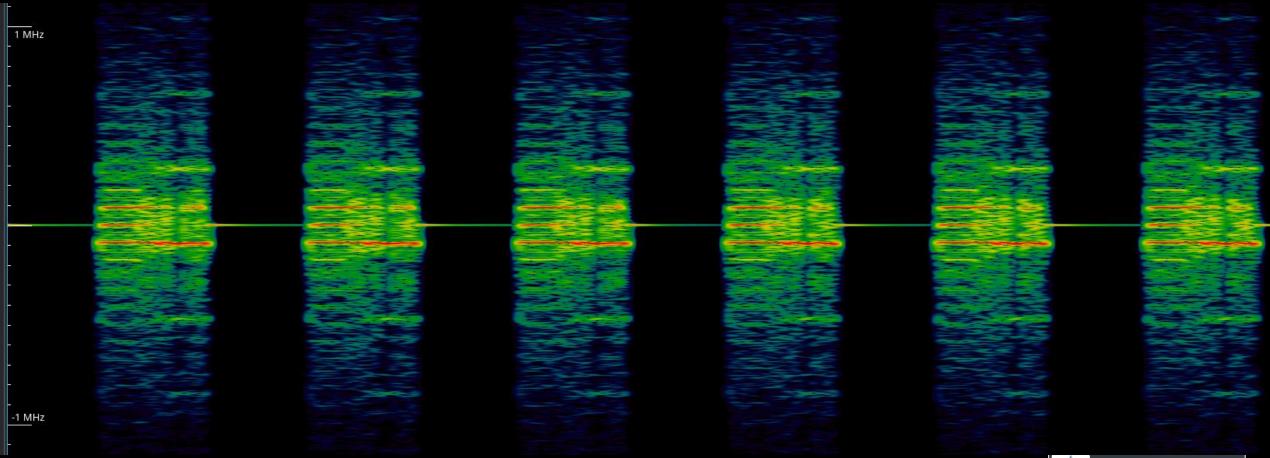
	~ : zsh — Konsole	~ ^ ×	2 >	×.				р	entest-windo	ows - VMwar	re Workstati	on				~ ^ ×
File Edit View Bookmarks Plugins Settings Help			File	Edit Vi	ew VM	Tabs Help										
		000000000000000000000000000000000000000	- E F	Pix Templ	late Desgin	C.									- C	ı ×
<pre>m ∧ ∧ hackrf_transfer -r[/tmp/old_pric b -a 1 -x 43 -l 16 -g 20</pre>	e -1 433264000 -5 4000000 -a 0	0000000000000000888690C337Ca01				12; 290:128*296; 42				7.0				Item Type:	Text	~
			Tag	g Size:	154	213 290	420	/50	1250	_ Hotate		Tag Color:	Red ~	Left:	1	
					e Sample:ES									Top:	1	
			P	rice	e: 5	\$								价格上下标 大小kr偏移。 9.98[priceSc	Value格式[price y偏移 分隔标点 pript[20]0,20].]	·Script字体]
															Price: 5\$	
														FontSize:	20	
														FontColor:	Black	~
														AntiColor:	False	
														FontFamily:		
														FontStyle: Alignment:	Regular Left	Ť
															N O H O	Transr 🗸
														VarKey:		~
														Format Flags:	NoClip	~
														ImageType:		~
														R 127 G	127 B 127 G	ray 127
		I												Cancel	Refresh	F5,Enter) Excel SaveA
			ID	Туре	X Y	VarValue	FontSize	AntiColor	FontFamily	FontStyle	Alignment	FontColor	Rectangle	Tag: 05B	6B6	0
			0	Text	1 1	Price: 5\$	20	False	SimSun	Regular	Left	Black	0 0 Transparer	00000000000	ver: 0 RSSI: -256	Temp: 0 🔺
														Station: 14 B 05B6B6 Pow 25 Result: Su Send Result:	OK ned result data:[1 latchCode:21415 ver: 2,9 RSSI: -2 uccess	TagID: Temp:
														058686 Pow	er: 2,9 RSSI: -2	Temp:
													Activa	25 Result: Su	ISCF114 V	Send
			<										Go to S		ctivate Wind	lows
				م -	Type he	ere to search			0	i Erg		Û		සී (10) ලි E	NG 05:59	22 🖵
			To ret	turn to v	our com	puter, move the	e mouse poir	nter outside	e or press Ci	rl-Alt.				8	R 1	a 🖹 🖻 🖺
· 🗎 💿 💿 🗗 💈 🖂			Ionet	i i i i i i i i i i i i i i i i i i i	our comp	acci, move the	e mouse poir	iter outside	e er press er			à 🗉 🎧 I	🕈 🏺 🖥 🖂			

Title: Self-Labeling Electronic Shelf Labels. | Responsible: S. Robertz | Version / Date: V1.0/2022-06 | Confidentiality Class: public © 2022 SEC Consult | All rights reserved



an atos company

The RF Protocol Determining the Correct Modulation



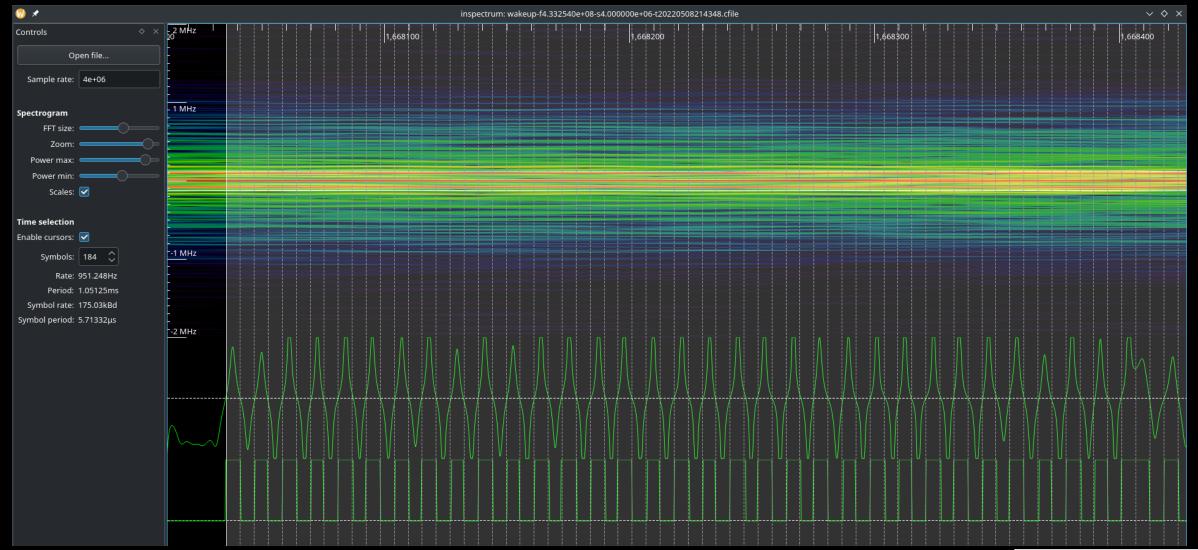
Title: Self-Labeling Electronic Shelf Labels. | Responsible: S. Robertz | Version / Date: V1.0/2022-06 | Confidentiality Class: public © 2022 SEC Consult | All rights reserved

27



an atos company

The RF Protocol Manually Decoding Frames





The RF Frames Activating the Tag

- 920 different frames, simply counting down to zero
- Each frame repeated 5 times
- Transmitted at 175 kBaud

Preamble	Sync Header	Frame Length	TagID	Fixed Value	Frame Counter	Fixed Value	CRC16
AAAAAAAA AAAAAA	D391D391	08	065302	0000	0398	Oa	2708



The RF Frames The Image Frame Structure

- Transmitted at 100kBaud
- Frame 1 out of 9
- Max 54 Byte of Image data
- Frame Length does not include CRC
- CRC creation starts at Frame Length field

Preamble	Sync Header			Frame Counter			CRC16
ААААААА ААААААА	00 0	3c	065302	0901	33	<image data="" structure=""/>	CRC

30

The RF Frames Special Image Frames

- Larger displays will require more than 256 frames
- First frame uses 16bit as frame counter
- Second frame starts with count zero and counts up towards the number transmitted in the first frame

Preamble	Sync Header	Frame Length	TagID	Frame Counter	Fixed Value	Payload	CRC16
AAAAAAA AAAAAAA	0000	3c	065302	<count></count>	33	<image data="" structure=""/>	CRC



The RF Frames

The Image Data Structure

- The image data structure starts with an additional header
- FC0000000 indicates black color channel
- FC8000000 indicates red color channel
- Second LED byte, 0b0111 to turn LED to white
 - One bit per color channel

				Compression header	Display Height		Payload
0700	BF75	OOED	000A	fc00000000	007f	0127	<compressed data="" image=""></compressed>



The RF Frames

The Image Compression

- 3 colors supported (white, black, red) \rightarrow 2bit per pixel
- Image payload too short for the amount of display pixel → custom compression algorithm is used
- Reverse Engineered from .NET SDK package (https://www.nuget.org/packages/eTag.SDK/)
- Uses Run-length encoding per color channel



The RF Frames The Image Compression

1/0

0

• Case 1: Less than 8 consecutive bits

1/0 1/0 1/0 1/0 1/0 1/0 1/0

Count

• Case 2: Less than 32 consecutive bits

Case 3: Less than 256 consecutive bits

1 1/0 0 0 0 0 0 0

Repeat [0:7]

• Case 4: Less than 2 ^ 16 consecutive bits

0 1/0 0 0 0 0 0 0

Repeat [8:15]

Repeat [0:7]



The RF Frames The Tag Response

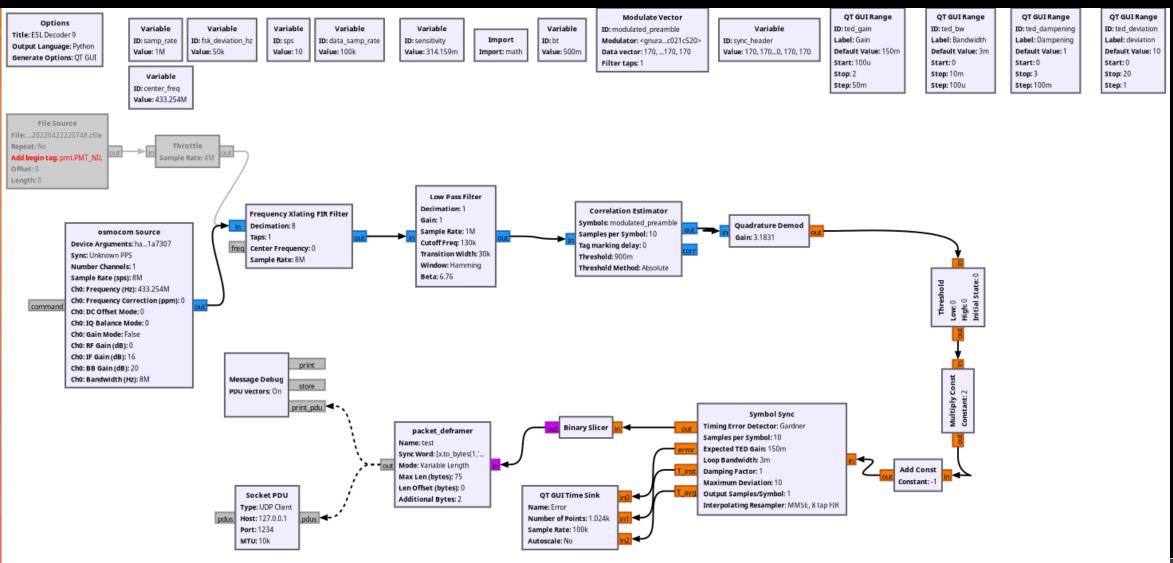
- Repeated 3 times
- 100kBaud

Sync Header		Frame Length	TagID	Battery Voltage	RSSI[1]	RSSI[0]	Temperature
AAAAAAAA AAAAAA	D391 D391	07	065302	1D = 2.9V	20	68	E9 = 23.3 C



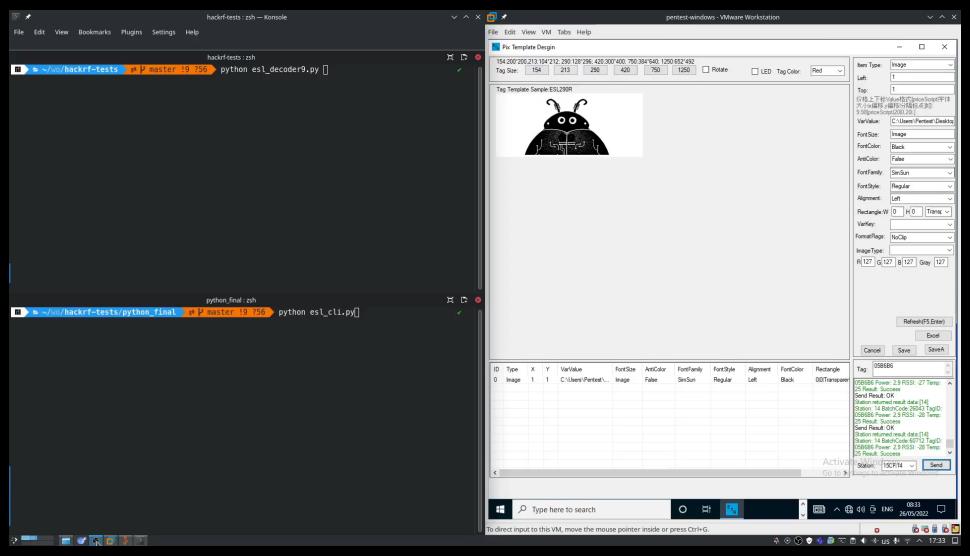
The RF Protocol

Receiving Images in GNU Radio





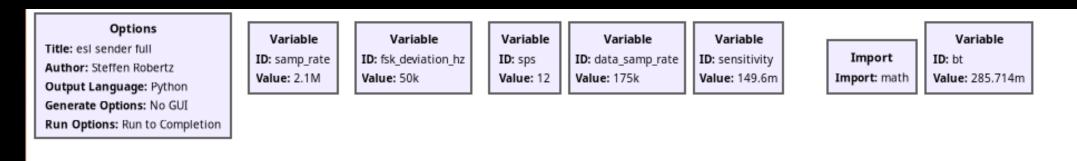
Live Demo Receiving Tag Information

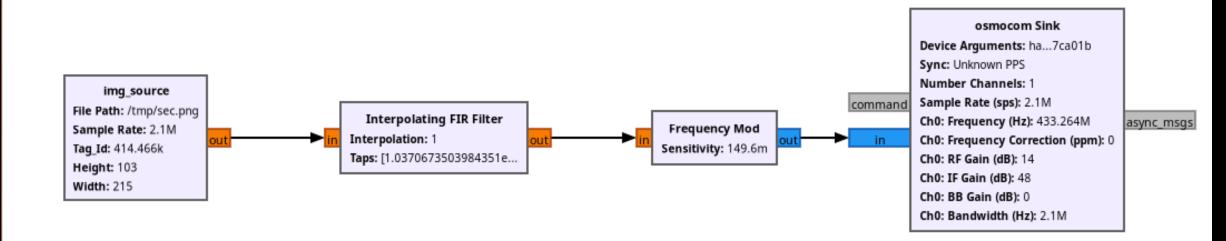




an atos company

The RF Protocol Sending Images With GNU Radio







Live Demo Modifying Tag Contents

File Edit View Bookmarks Plugins Settings Hel

🖬 🕨 🗢 /workspace/hackrf-tests 🛛 🕸 🖗 master !9 ?56 🖉 python esl_sender_full.py[]



~: zsh hackrf-tests : zsh





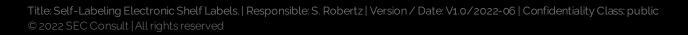
Conclusion

- Identified unknown MCU
- Gained access via debug port
- Confirmed replay vulnerability
- Reverse engineered the RF protocol
 - Gained ability to send and receive valid frames
- Able to receive and decode ESL price updates
- Able to change tag content to arbitrary information
- Range limited by RF power



Conclusion Lessons Learned

- Protocol does not contain any security measures
- Custom protocols at 433 MHz do not increase security
 - Can be received and impersonated with e.g. a C1101 (2\$)
- Protocol robustness could have been increased by using error correction algorithms
- Relabeling a MCU does not protect against finding the correct MCU family
- All code will be released on <u>GitHub</u> within the next weeks



41



Do you have any further questions?

Don't hesitate to contact us: <u>s.robertz@sec-consult.com</u>

www.sec-consult.com

Title: Self-Labeling Electronic Shelf Labels. | Responsible: S. Robertz | Version / Date: V1.0/2022-06 | Confidentiality Class: public © 2022 SEC Consult | All rights reserved



