Arash Token – Iranian Patent # 82305

Author (s): Hamidreza Noursalehi – CEO & Founder / Inventor **Date:** August 24, 2014

Version: 1 - Demo

USE CASE NAME:	**فرايند هاي مربوط به احراز هويت و امضای تراکنشهای ادرای و مالی با توکن آرش – لایه DMZ**	**USE CASE TYPE**
USE CASE ID:	0	Abstract: ☑
PRIORITY:	1	*Extension:* ☐
INVOKED BY:	واحد فن آوری اطلاعات انواع سازمانهای دولتی و خصوصی – امنیت داده ها و شبکه	
PARTICIPATING ACTORS:	مدیران، سرپرست شبکه، کارکنان و مشتریان	
DESCRIPTION:	سیستم متمرکز احراز هویت با توکن پیشرفته آرش	
PRE-CONDITION:	اقدام به پیاده سازی زیر ساخت فن آوری اطلاعات	
TYPICAL COURSE OF EVENTS:	1- اقدام برای ورود به سیستم - لایه DMZ	
	2- احراز هویت – Authentication	
	3- مجوز دسترسی - Authorization	
ALTERNATE COURSES:	به روز رسانی دوره ای کلیدهای نامتقارن و متقارن هر کاربر	
POST-CONDITION:	افزودن انواع فاکتورهای امنیتی بر مبنای تهدیدهای گزارش شده	

Arash Token – Iranian Patent # 82305

Author (s): Hamidreza Noursalehi – CEO & Founder / Inventor **Date:** August 24, 2014

Version: 1 - Demo

USE CASE NAME:	**اقدام برای ورود به سیستم – لایه DMZ**	**USE CASE TYPE** **Business Requirements: ☑**
USE CASE ID:	0.1.1	
PRIORITY:	2	
SOURCE:	Flowchart – Patent 82305 – Fig. 7 proceed_to_login.asp	
PRIMARY BUSI-NESS ACTOR:	کاربر سیستم	
OTHER PARTICI-PATING ACTORS:	سرپرستی شبکه ، مدیریت امور سیستمها	
OTHER INTER-ESTED STAKE-HOLDERS:	توسعه سیستمها	
DESCRIPTION:	ارزشیابی و امکانسنجی محیطی بر مبنای ماهیت کاربر در لایه DMZ	
PRE-CONDITION:	نام کاربری در سیستم ثبت شده باشد	
TRIGGER:	کاربر در سیستم عضو میشود – Sign up	
TYPICAL COURSE OF EVENTS:	**Actor Action**	**System Response**
	Step 1:	**Step 2**:
	کاربر برای ورود به سیستم اقدام میکند	سیستم نام کاربری را از کاربر درخواست میکند
	کاربر نام کاربری را وارد میکند.	سیستم وضعیت نام کاربری وارد شده را به لحاظ نوع احراز هویت تعیین شده (رمز ثابت – فقط با توکن – دو عاملی) کنترل میکند.
ALTERNATE COURSES:	وابسته به نوع شرایط حاکم بر شبکه همچون قطع ارتباط با سیستم متمرکز CA & CMZ در لحظه اقدام برای ورود به سیستم، به لحاظ احراز هویت، لایه DMZ میتواند تصمیم بگیرد که راسا نسبت به احراز هویت عمل کند.	
CONCLUSION:	نام کاربری در سیستم موجود است و نوع احراز هویت تعیین شده تعیین میگردد.	
POST-CONDITION:	احراز هویت	
BUSINESS RULES	هر نام کاربری میتواند به سادگی و بدون ایجاد ضرب اطلاعات در سطح کل سیستمهای نرم افزاری، در هر لایه DMZ ثبت نام کرده و وابسته به سیاستهای تعریف شده، خدمات مورد نظر را دریافت نماید. هر نام کاربری میتواند به طور کلی از سیستم مرکزی مدیریت، تایید و یا قطع شود. در اینصورت در هیچ یک از دیگر DMZ ها قادر به	

	سرویس گرفتن نخواهد بود. همچنین، یک کاربر ممکن است فقط در یک لایه DMZ از دریافت خدمات محروم شود ولی همچنان توسط سایر لایه ها خدمات دریافت کند. این مهم از منظر هدایت کاربرای در شبکه مبتنی بر پردازش ابری بسیار حائز اهمیت است.
IMPLEMENTATION CONTRAINTS AND SPECIFICATIONS	ارتقاء نحوه عملکرد مستقل لایه های DMZ متفاوت به یک سیستم متمرکز مرکزی
	تجهیز کاربران به توکن های سخت افزاری
OPEN ISSUES:	طراحی سیستمهای پس پردازش در تشخیص تقلب و رخنه در سیستم بر مبنای گزارش از سوابق ورود کاربران به سیستم

Arash Token – Iranian Patent # 82305

Author (s): Hamidreza Noursalehi – CEO & Founder / Inventor **Date:** August 24, 2014

Version: 1 - Demo

USE CASE NAME:	**Authentication – احراز هویت**	**USE CASE TYPE** **System Analysis:** ☑
USE CASE ID:	0.1.2	
PRIORITY:	1	
SOURCE:	Flowchart – Patent 82305 – Fig. 6 Authentication.asp crypto_functions/ rsa_64bit_encrypt.asp	
PRIMARY BUSINESS ACTOR:	مدیریت امور سیستمها	
OTHER PARTICIPATING ACTORS:	سرپرستی شبکه ، کاربر سیستم	
OTHER INTERESTED STAKEHOLDERS:	مدیریت توسعه سیستمها	
DESCRIPTION:	احراز هویت کاربر سیستم	
PRE-CONDITION:	نام کاربری و شرایط احراز هویت توسط سیستم دریافت شده است	
TRIGGER:	رمز عبور در سیستم ثبت میشود	
TYPICAL COURSE OF EVENTS:	**Actor Action**	**System Response**
	Step 1:	**Step 2**:
	نام کاربری در سیستم وارد شده و کلید ادامه فشرده میشود	سیستم بر مبنای شرایط احراز هویت با: رمز عبور ثابت (0)، فقط توکن (1) یا دو عاملی(2) مواجه میشود و بر حسب آن (0 و 2) از کاربر کلمه عبور ثابت را میپرسد یا آنرا نادیده میگیرد. همچنین، سیستم بر حسب در نظر گرفتن توکن (1 و 2) یک عبارت تحت عنوان چالش به کاربر نمایش میدهد.
	کاربر رمز عبور ثابت خود را وارد میکند یا نمیکند. کاربر چالش تعیین شده توسط سیستم را در توکن خود وارد میکند یا نمیکند.	سیستم در لایه DMZ نام کاربری را به سیستم CA منتقل میکند و پاسخ آنرا که حاوی کلید عمومی و وضعیت فعال (1) یا غیر فعال (0) یا موجود نیست (-1) را دریافت میکند. سپس اقدام به محاسبه مقدار پیغام مخفی جلسه کاری با فرمول

		زیر مینماید: msg = chall_1 * chall_2 msg = msg + chall_3 + … + chall_n msg = msg + factor_N msg_value_str= right (msg, 5) سپس مقدار پیغام را با کلید عمومی و از طریق الگوریتم RSA رمز کرده و مقدار رمز شده را به سیستم CMZ ارسال میکند و با استفاده از کلید خصوصی کاربر که به صورت کاملا محرمانه از آن نگهداری میشود، اقدام به رمزگشایی و درستیابی به مقدار پیغام جلسه کاری مورد نظر کرده و سپس آنرا مجددا با کلید خصوصی خود رمز میکند و سپس از آن یک رمز عبور موقت یکبار مصرف تولید کرده و برای سیستم DMZ ارسال میکند. سیستم DMZ و در ادامه، با مقایسه مقدار رمز عبور ثابت و رمز عبور موقت که کاربر توسط توکن خود تولید کرده است، با مقادیر موجود در بانک اطلاعاتی در DMZ و مقدار ارسالی از CMZ اقدام به احراز هویت میکند.
ALTERNATE COURSES:	لایه DMZ میتواند ضمن در نظر گرفتن CMZ ، جهت اختصاصی کردن احراز هویت اقدام به تولید و جابجایی یک Pre-Shared Key بین خود و توکن کاربر نماید. این مهم باعث میگردد لایه DMZ اطاعت کورکورانه از CMZ نداشته باشد.	
CONCLUSION:	کاربر به صفحات کاربری وارد میشود یا از ورود منع میشود.	
POST-CONDITION:	مجوز دسترسی - Authorization	
BUSINESS RULES	به این ترتیب، لازم نیست در ازای هر سرویس یا سیستم DMZ که در سطح سازمانی ایجاد میگردد، کاربران را مجبور به خرید و نگهداری از یک توکن سخت افزاری جدید نماییم.	
IMPLEMENTATION CONTRAINTS AND SPECIFICATIONS	پیروی سیستم احراز هویت متمرکز آرش از یک استاندارد منتشر نشده.	
	نیاز محافظت شدید و کامل از CMZ با ایجاد یک سرور میانی تحت عنوان Content Inspector که به نحوی داده های منتقل شده بین CMZ & DMZ را کنترل میکند	
OPEN ISSUES:	ارتقاء عملکرد سیستم CMZ به سمت یک HSM	

Arash Token – Iranian Patent # 82305

Author (s): Hamidreza Noursalehi – CEO & Founder / Inventor **Date:** August 24, 2014

Version: 1 - Demo

USE CASE NAME:	**Authorization – مجوز دسترسی**	**USE CASE TYPE** **Business Requirements: ☑**
USE CASE ID:	0.2.1	
PRIORITY:	3	
SOURCE:	Flowchart – Patent 82305 – Fig. 6 Authorization.asp crypto_functions/ rsa_64bit_encrypt.asp	
PRIMARY BUSI-NESS ACTOR:	مدیریت امور سیستمها	
OTHER PARTICI-PATING ACTORS:	شبکه شاپرک، سرپرستی شبکه ، کاربر سیستم	
OTHER INTER-ESTED STAKE-HOLDERS:	مدیریت توسعه سیستمها ، بانک مرکزی	
DESCRIPTION:	امضای دیجیتال و کنترل مجوز دسترسی	
PRE-CONDITION:	مرحله احراز هویت با موفقیت انجام شده باشد	
TRIGGER:	تراکنشهای حساس مالی و اداری به اجرا در می آیند	
TYPICAL COURSE OF EVENTS:	**Actor Action**	**System Response**
	Step 1:	**Step 2**:
	کاربر اقدام به انتقال وجه به حساب کاربر دیگری مینماید.	سیستم مشخصات شماره حساب کاربر مقصد و مبلغ مورد نظر جهت انتقال را از کاربر میپرسد.
	کاربر مشخصات شماره حساب کاربر مقصد و مبلغ مورد نظر جهت انتقال را وارد میکند	سیستم از مبلغ و شماره حساب مقصد ، یک مقدار چالش استخراج میکند و به کاربر نمایش داده و منتظر دریافت پاسخ می ماند.
	کاربر مقدار چالش را در توکن خود وارد کرده و یک پاسخ دریافت کرده، آنرا در سیستم وارد میکند.	سیستم مقدار چالش را به سبک مرحله احراز هویت با کمک CA & CMZ به امضای دیجیتال تبدیل کرده و با مقدار وارد شده توسط کاربر مقایسه میکند. در صورت تایید، تراکنش مالی یا اداری اجرا میشود.

ALTERNATE COURSES:	شماره حساب مبدا و آدرس IP و سایر مشخصات در تولید چالش دخالت داده میشوند. برای رقمهای پائین ، شاید سیستم تصمیم بگیرد که احتیاج به امضای دیجیتال تراکنش با توکن نباشد.	
CONCLUSION:	تراکنش های حساس مالی و اداری به اجرا در می آیند.	
POST-CONDITION:	اجرای سیستم احراز هویت متمرکز آرش در نسخه اصلی	
BUSINESS RULES	تراکنش های حساس مالی و اداری در سازمانها،ادارات و بانکها و موسسات مالی و اعتباری به شدت محافظت میگردد، به نحوی که با یک توکن غیر متصل (Air-Gap) – در صورت حفظ شرایط خاص در تولید توکن ها - امضای دیجیتال واقعی و در غیر اینصورت شبه امضای دیجیتال صادر میگردد.	
IMPLEMENTATION CONTRAINTS AND SPECIFICATIONS	زمانبر شدن مراحل تولید امضاء با توکن در صورت زیاد شدن تعداد تراکنشها	
	قطع یا عدم دسترسی امضاء کننده به شبکه	
OPEN ISSUES:	تعداد زیاد تراکنشها به نحوی بافر شده و در نهایت یک پالش برای همه آنها استخراج شده و همزمان با یک امضاء همه آنها اجرا میشوند.	