IPAACA - Feature #464

Feature # 466 (New): IPAACA v3

v3: Sender tokens

2016-02-16 14:23 - Ramin Yaghoubzadeh

Status:	New	**Start date:**	2016-02-16
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

In lieu of a complete authentication / encryption layer, v3 will include a simple token-based filtering mechanism, probably defaulting to a username-derived personal token. Components can override their sending token, and also the default filter of allowing reception of IU events with the user's token only.
In so doing, basic concurrent usage of different users / demos is made feasible – while not excluding the possibility to wantonly modify a closed system when required.

History

#1 - 2016-02-16 14:29 - Ramin Yaghoubzadeh

- Parent task set to #466

#2 - 2016-03-15 19:54 - Ramin Yaghoubzadeh

Maybe use digests of some user-only readable secret?
One could also use a digest of some user-only-readable secret (like .Xauthority??) - but no real gain since eavesdropping is 100% open (locally, at the very least).

Linux
md5sum ~/.Xauthority | cut -d' ' -f1

Mac
md5 -q ~/.Xauthority

(or preferably use a portable library's MD5 or something, linked internally in all ipaaca versions).